ISA Server 2004

Inhaltsverzeichnis:

Installation des ISA Server 2004 deutsch auf Windows Server 2003 3
Aktivierung der Webcachefunktion beim ISA Server 2004 15
Erkennung von Eindringversuchen und DNS-Angriffen aktivieren 22
ISA Server 2004 als reinen Webproxyserver konfigurieren 27
Bestimmte WebSeiten nicht cachen 35
Verteilen der Webproxy-Einstellungen per Gruppenrichtlinie 42
Socket Pooling bei Windows Server 2003 und ISA Server 46
DNS Auflösung 49
Geplante Inhaltsdownloadsaufträge einrichten 54
Benutzerauthentifizierung bei ausgehenden Webanfragen 60
RADIUS/IAS Authentifizierung mit dem ISA Server 2004 65
SMTP-Anwendungsfilter 76
Erstellen eines neuen Netzwerkes 85
ISA Server 2004 – Erstellen einer Webverkettung (Proxy-Chain) 95
Microsoft ISA Server 2004 95
ISA Server 2004 – Mehrfachnetzwerke - Besonderheiten 102
ISA Server 2004 – IP-Einstellungen definieren 110
Konfiguration des ISA für automatische Suche der Clienteinstellungen (WPAD/WSPAD) 115
Benutzerrollen und -berechtigungen delegieren 125
Backup und Restore eines ISA Server 2004 130
Remoteverwaltung eines ISA Server 2004: Teil 1 - Remotedesktop (RDP) 135
Remoteverwaltung eines ISA Server 2004: Teil 2 - Managementkonsole (MMC) 141
ISA Info - >Das< Dokumentations- und Supporttool für den ISA Server 2004 150
Schönheitskorrektur: SQL Server-Dienst Manager 157
Erstellen einer Firewallrichtlinie am Beispiel von POP3 159
Systemrichtlinien: Firewallrichtlinien für den ISA Server selber 168
Ein- und Ausgehende ping-Anfragen konfigurieren 176
Zugriff auf Windowsupdate V5 durch den ISA 2004 - Von Christian Gröbner 183
ISA Server 2004 – Microsoft SQL Server Veröffentlichung 195
Einrichtung von RPC over HTTPS mit dem ISA Server 2004 200
Zeitabgleich mit einem externen Zeitserver 229
Outlook Webaccess per SSL mit Formsbased Authentification mit dem ISA 2004 238
ISA Server 2004 – HTTP Filter 263
Konfiguration des ISA Server zur Unterstützung interner Mailclients (z.B. Outlook/Outlook Express) 274

Veröffentlichen von Remotedesktop zur Verwaltung des ISA Server Computers 279
Veröffentlichen eines internen Terminalserver oder interner Remotedesktop Services 287
Übersicht über die ISA Server 2004 Monitoring Funktionen 303
Konfiguration einer Konnektivitätsverifizierung 313
Alarmkonfiguration 320
ISA Server 2004 – Protokollierung 332
ISA Server 2004 – System Hardening 343
Toolbox - "Werkzeugkasten" für Firewallrichtlinien 358
Erstellen eines neuen benutzerdefinierten Protokollelementes in der Toolbox 360
Firewallrichtlinien 364
Erstellen und verwenden von Zeitplänen 367
ISA Server Clients - Teil 1: Der SecureNAT-Client 373
ISA Server Clients - Teil 2: Der Firewall Client 376
ISA Server Clients - Teil 3: Der Webproxyclient 392
Eingehende VPN-Verbindungen per PPTP 397
ISA Server 2004 – Site–to–Site VPN mit L2TP/IPSec 409
ISA Server 2004 – VPN Client Zugang mit PPTP 426
ISA Server 2004 – VPN Quarantine Control 438
Clientkonfiguration für PPTP-VPN-Verbindungen mit PocketPC 2002 448
Clientkonfiguration für PPTP-VPN-Verbindungen mit Windows 2000/XP 454
Einrichten einer Internetanbindung über eine DFÜ Verbindung 459
SMTP/POP3 ausgehend nicht möglich 469

Installation des ISA Server 2004 deutsch auf Windows Server 2003

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004 RTM

Die Version 2004 unterscheidet sich wesentlich vom ISA Server 2000. Zu den Unterschieden und Neuerungen wird es hier demnächst separate Artikel geben.

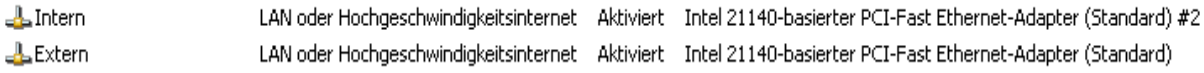
Was sich nicht geändert hat, sind die Betriebssystemseitigen Voraussetzungen. Der ISA Server 2004 unterstützt folgende Serverbetriebssysteme und kann auf ihnen installiert werden:

- Windows 2000 Server mit Servicepack 4
- Windows 2000 Advanced mit Server Servicepack 4
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition

Es wird jedoch empfohlen, Windows Server 2003 als Grundlage zu verwenden. Die Artikel der msisafaq.de beziehen sich prinzipiell immer auf Windows Server 2003, sofern nicht anders angegeben wird.

Vor der Installation von ISA Server 2004 muss das Betriebssystem entsprechend konfiguriert und vorbereitet werden. Dazu gehört u.a. dass alle verfügbaren Hotfixe eingespielt werden. Als nächstes muss die Netzwerkkonfiguration vorgenommen werden. Damit sämtliche Funktionen des ISA genutzt werden können, benötigt der Server 2 Netzwerkschnittstellen in 2 unterschiedlichen IP Subnetzen.

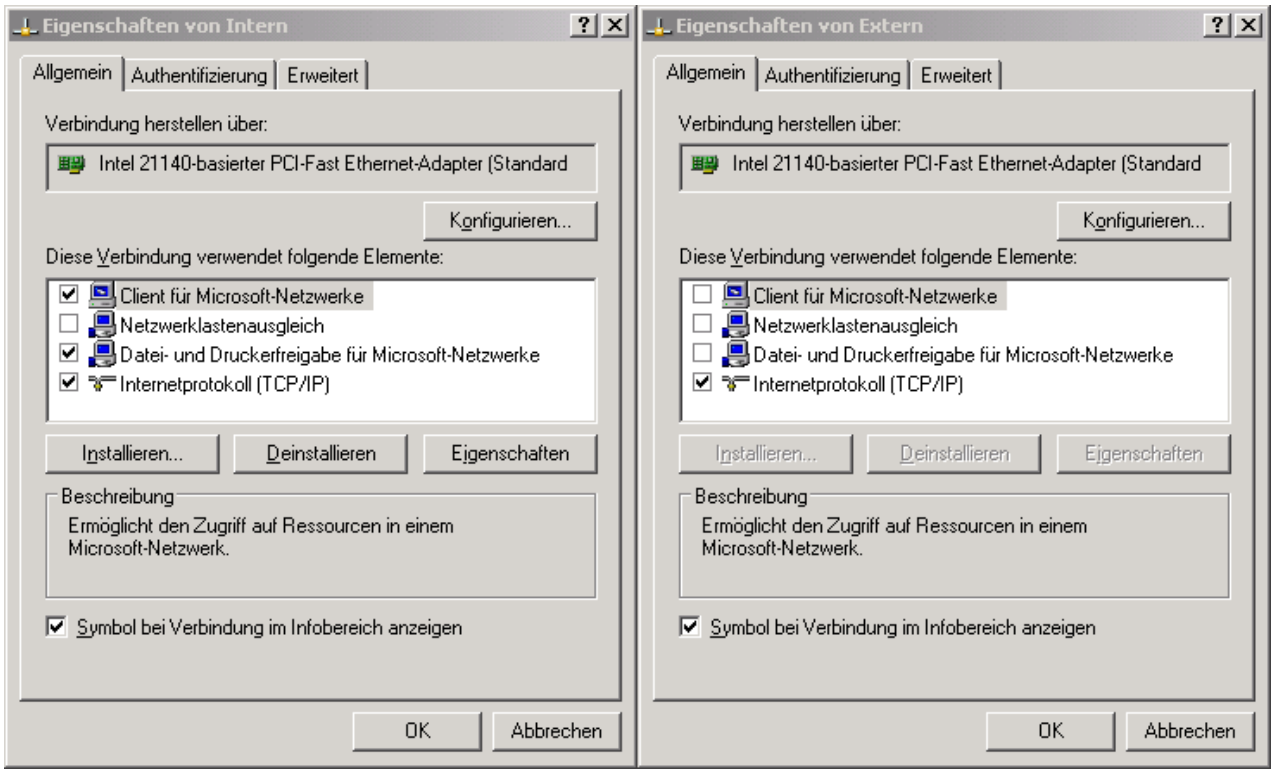
Für diesen Artikel verwende ich einen Windows Server 2003 mit folgender Netzwerkkonfiguration:



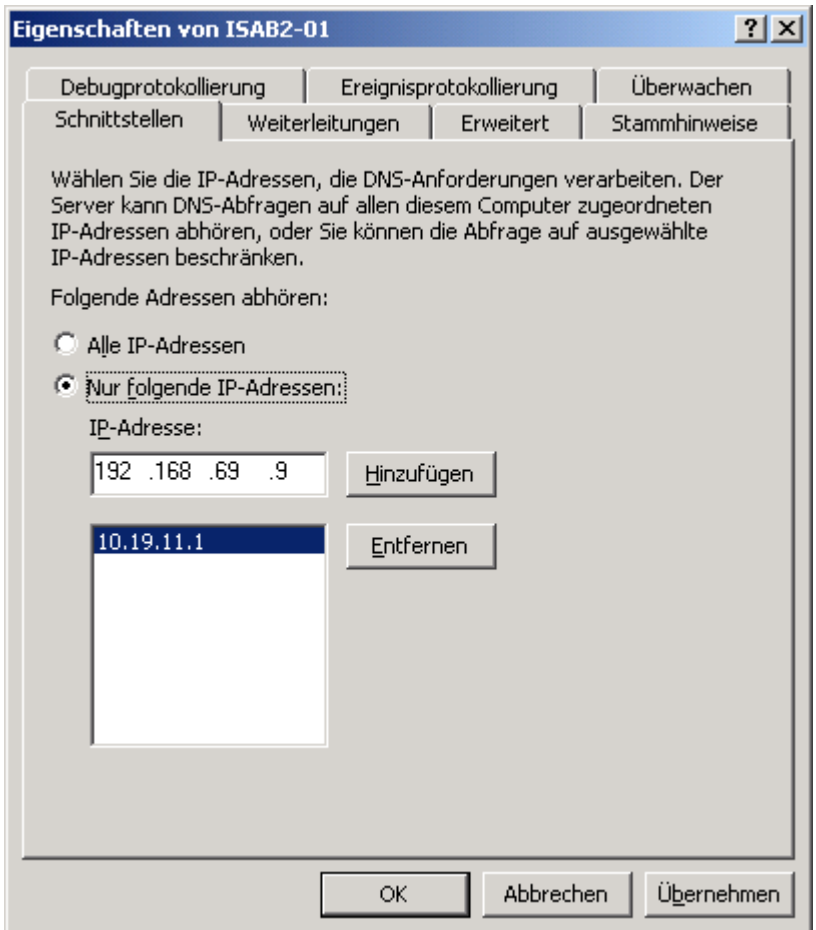
Intern	LAN oder Hochgeschwindigkeitsinternet	Aktiviert	Intel 21140-basierter PCI-Fast Ethernet-Adapter (Standard) #2
Extern	LAN oder Hochgeschwindigkeitsinternet	Aktiviert	Intel 21140-basierter PCI-Fast Ethernet-Adapter (Standard)

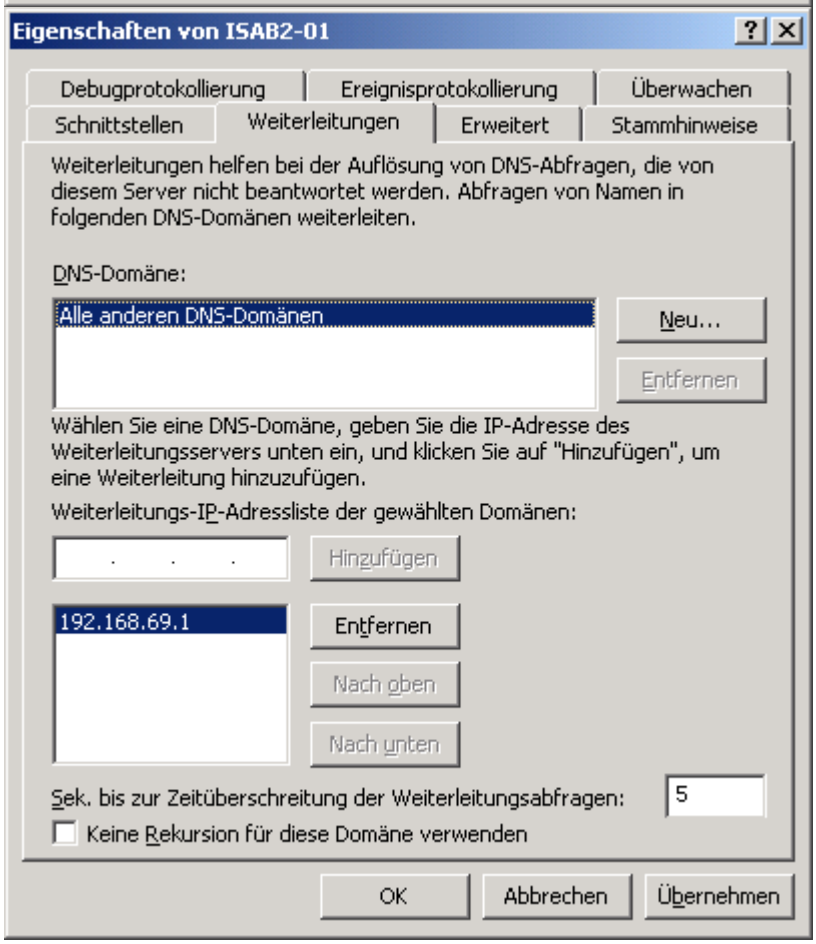
```
C:\>ipconfig /all

Windows-IP-Konfiguration

Hostname . . . . . . . . . . . . . : ISA2004-003
Primäres DNS-Suffix . . . . . . . .: msisafaq.de
Knotentyp . . . . . . . . . . . . .: Unbekannt
IP-Routing aktiviert . . . . . . . : Nein
WINS-Proxy aktiviert . . . . . . . : Nein

Ethernet-Adapter Intern:

Verbindungsspezifisches DNS-Suffix:
Beschreibung . . . . . . . . . . . : Intel 21140-basierter PCI-
Fast Ethernet-Adapter (Standard) #2
Physikalische Adresse . . . . . . .: 00-03-FF-FA-FF-FF
DHCP aktiviert . . . . . . . . . . : Nein
IP-Adresse. . . . . . . . . . . . .: 10.19.11.1
Subnetzmaske . . . . . . . . . . . : 255.255.255.0
Standardgateway . . . . . . . . . .:
DNS-Server . . . . . . . . . . . . : 192.168.69.1

Ethernet-Adapter Extern:

Verbindungsspezifisches DNS-Suffix:
Beschreibung . . . . . . . . . . . : Intel 21140-basierter PCI-
Fast Ethernet-Adapter (Standard)
Physikalische Adresse . . . . . . .: 00-03-FF-91-60-6D
DHCP aktiviert . . . . . . . . . . : Nein
IP-Adresse. . . . . . . . . . . . .: 192.168.69.9
Subnetzmaske . . . . . . . . . . . : 255.255.255.0
Standardgateway . . . . . . . . . .: 192.168.69.1
NetBIOS über TCP/IP . . . . . . . .: Deaktiviert
```

Folgende Netzwerkprotokolle sind an die jeweilige Netzwerkkarte gebunden:

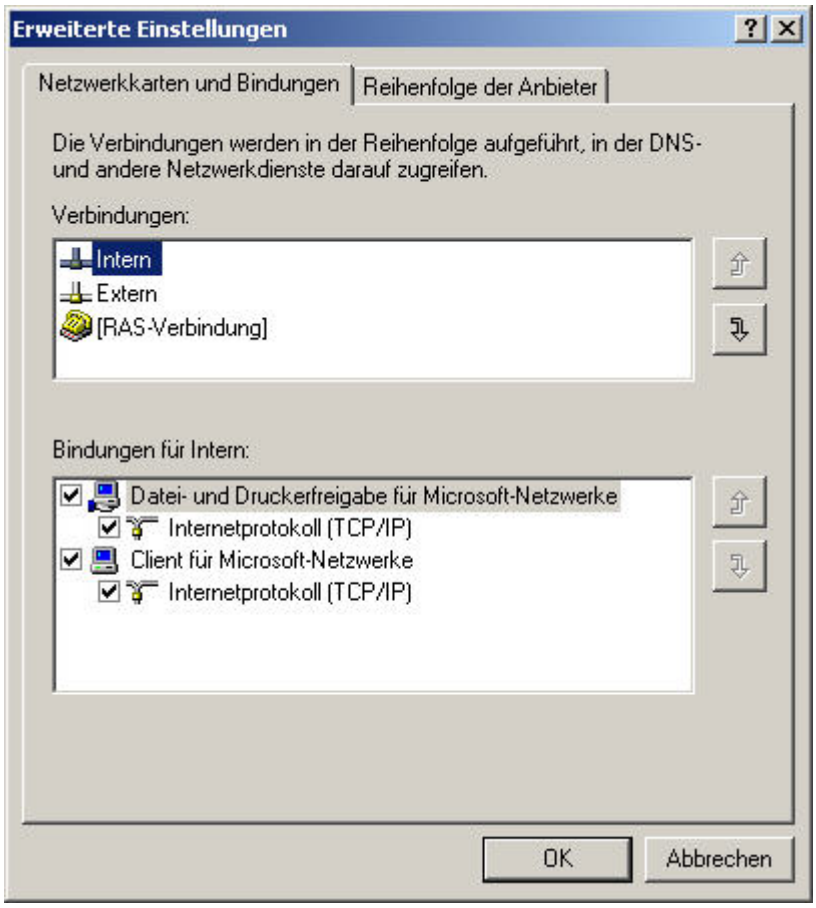


Auf dem ISA Server ist ein DNS Server installiert, der alle Anfragen an die IP-Adresse 192.168.69.1 weiterleitet. Der DNS Server hält keine Zone. Je nach Netzwerkumgebung kann er aber ein Backup der AD-integrierten Zone halten. Mehr zu DNS gibt es hier.

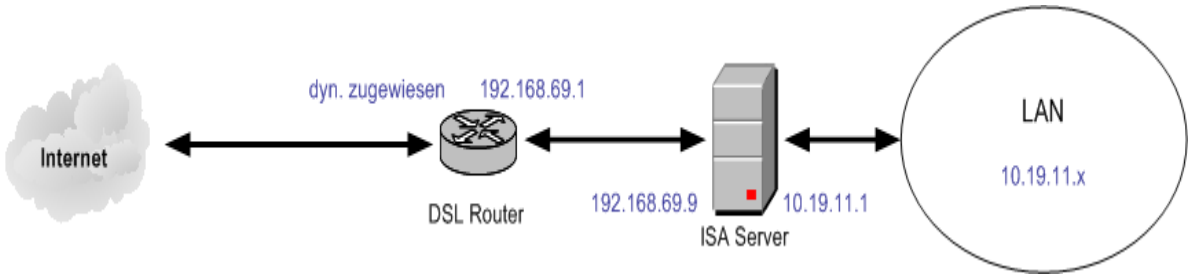

Eigenschaften von ISAB2-01
Debugprotokollierung
Ereignisprotokollierung
Überwachen
Schnittstellen
Weiterleitungen
Erweitert
Stammhinweise
Wählen Sie die IP-Adressen, die DNS-Anforderungen verarbeiten. Der Server kann DNS-Abfragen auf allen diesem Computer zugeordneten IP-Adressen abhören, oder Sie können die Abfrage auf ausgewählte IP-Adressen beschränken.
Folgende Adressen abhören:
Alle IP-Adressen
Nur folgende IP-Adressen:
IP-Adresse:
192 .168 .69 .9
Hinzufügen
10.19.11.1
Entfernen
OK
Abbrechen
Übernehmen


Eigenschaften von ISAB2-01
Debugprotokollierung
Ereignisprotokollierung
Überwachen
Schnittstellen
Weiterleitungen
Erweitert
Stammhinweise
Weiterleitungen helfen bei der Auflösung von DNS-Abfragen, die von diesem Server nicht beantwortet werden. Abfragen von Namen in folgenden DNS-Domänen weiterleiten.
DNS-Domäne:
Alle anderen DNS-Domänen
Neu...
Entfernen
Wählen Sie eine DNS-Domäne, geben Sie die IP-Adresse des Weiterleitungsservers unten ein, und klicken Sie auf "Hinzufügen", um eine Weiterleitung hinzuzufügen.
Weiterleitungs-IP-Adressliste der gewählten Domänen:
Hinzufügen
192.168.69.1
Entfernen
Nach oben
Nach unten
Sek. bis zur Zeitüberschreitung der Weiterleitungsabfragen:
5
Keine Rekursion für diese Domäne verwenden
OK
Abbrechen
Übernehmen

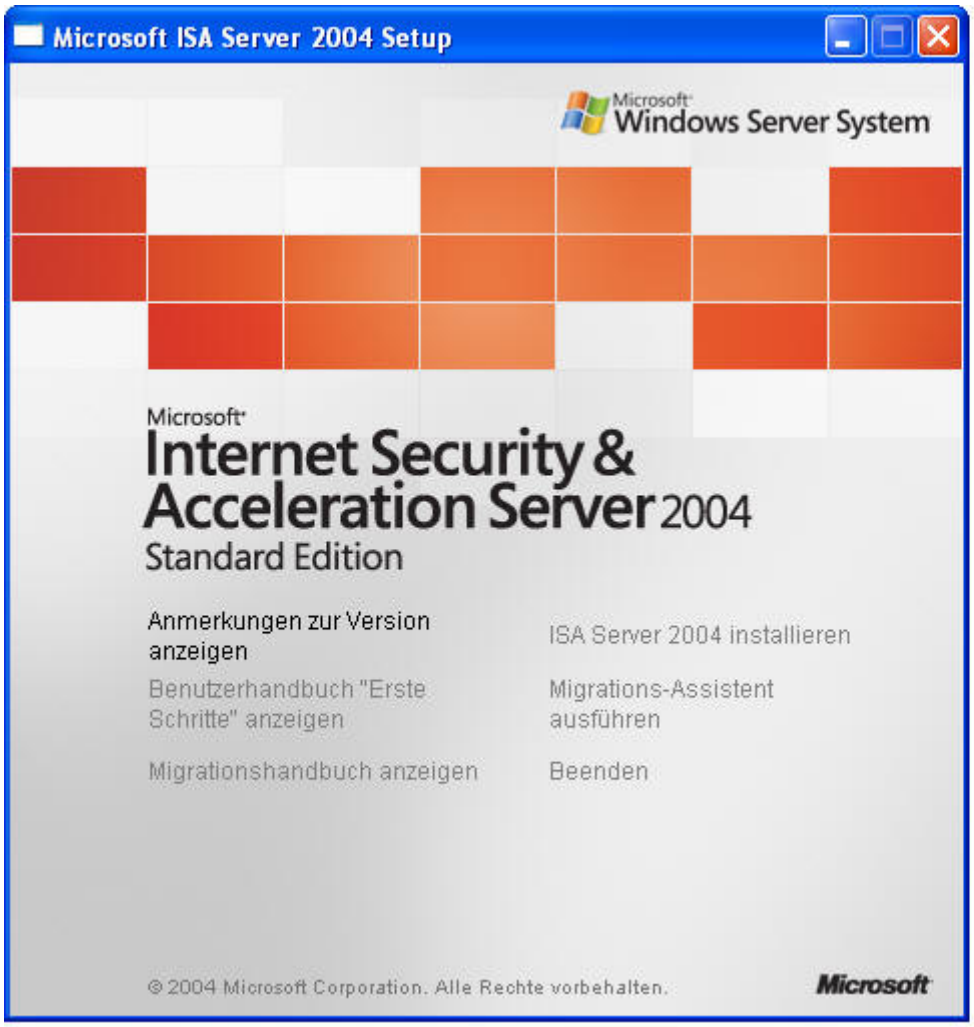
Der letzte wichtige Punkt bei der Vorbereitung des Betriebssystems ist die Bindungsreihenfolge der Netzwerkkarten:



Der Windows Server ist wie folgt an das Internet angebunden:



Nachdem nun alle Voraussetzungen erfüllt sind, kann die Installation des ISA Server 2004 beginnen:



Einen Blick in die Anmerkungen bzw. ins Benutzerhandbuch zu werfen schadet nie.

Für die Installation der Testversion bitte "ISA Server 2004 installieren" auswählen. Nach dem akzeptieren der Lizenzbedingungen (EULA) und der Eingabe der Produkt ID kommt man zu folgendem Auswahlfenster:

Die Typische Installation beinhaltet:

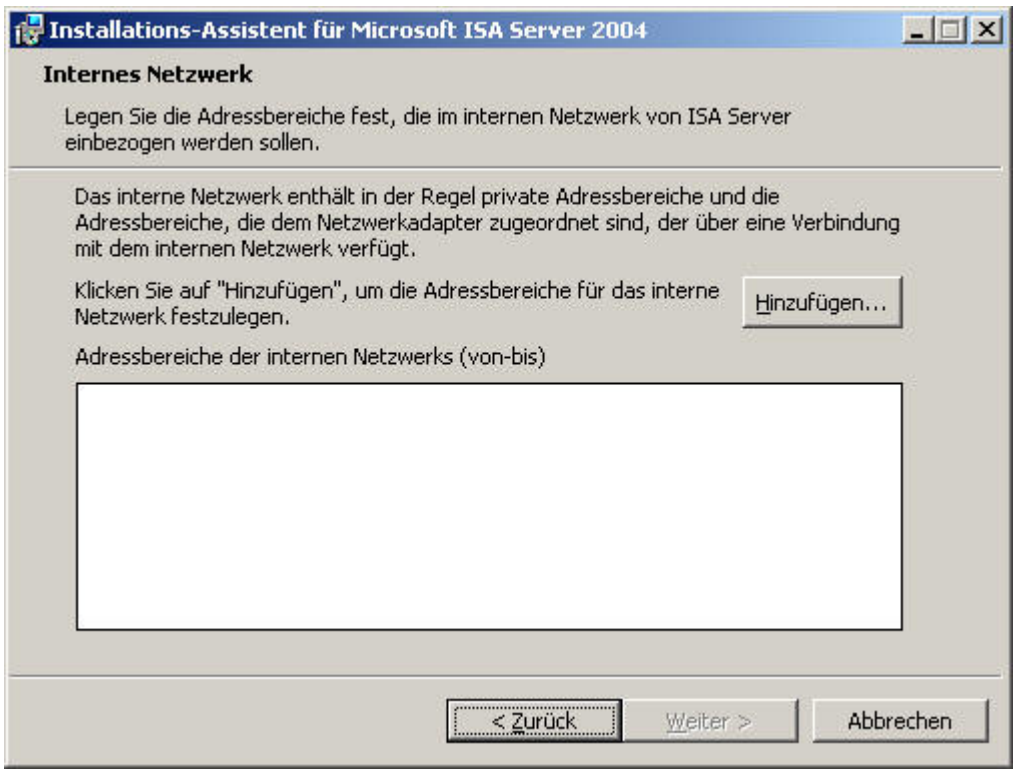
- Firewalldienste
- Erweiterte Protokollierung
- ISA Server-Verwaltung
- Installationsfreigabe für Firewallclient
-

Bei der Vollständigen Installation ist zusätzlich noch ausgewählt:

- Nachrichtenüberwachung

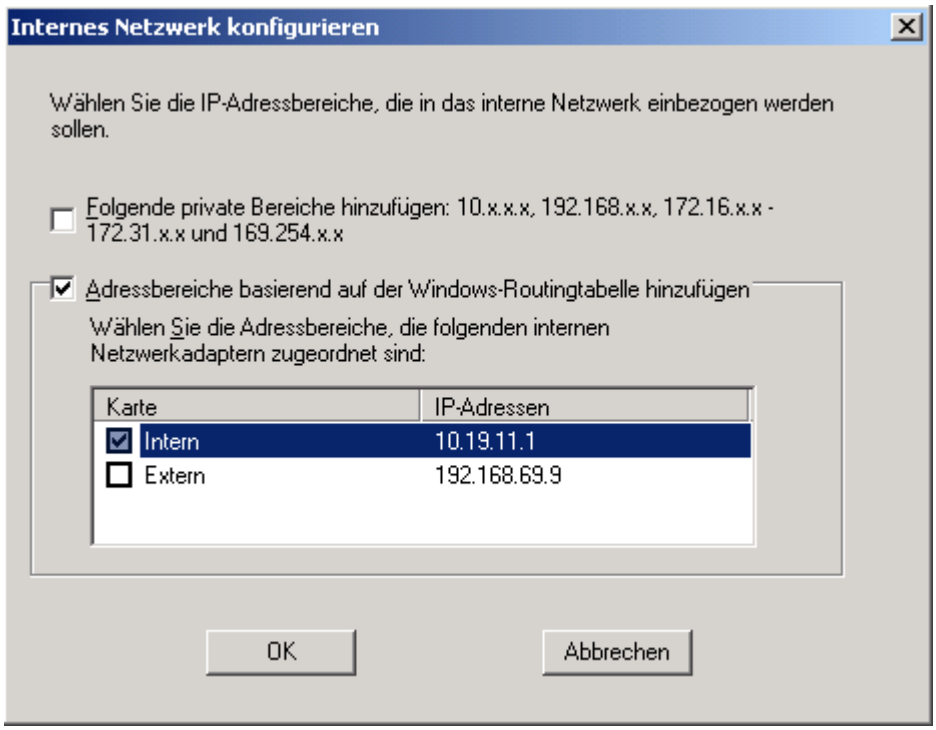
Die Installationsfreigabe für Firewallclient muss nicht zwingend auf dem ISA Server installiert werden. Hier ist ein wesentlicher Unterschied zum ISA Server 2000 erkennbar. Dort musste der Firewallclient immer zwingend von der \mspclnt-Freigabe am ISA Server installiert werden. Beim 2004er kann diese Freigabe auch auf einem internen Fileserver liegen. Warum? Der ISA Server 2004 kann das interne Interface (also die Schnittstelle zum LAN) komplett blocken und nur einige wenige zugelassene Protokolle durchlassen. Somit könnte man bei gesperrtem Filezugriff auf den ISA Server keinen Firewallclient mehr installieren.

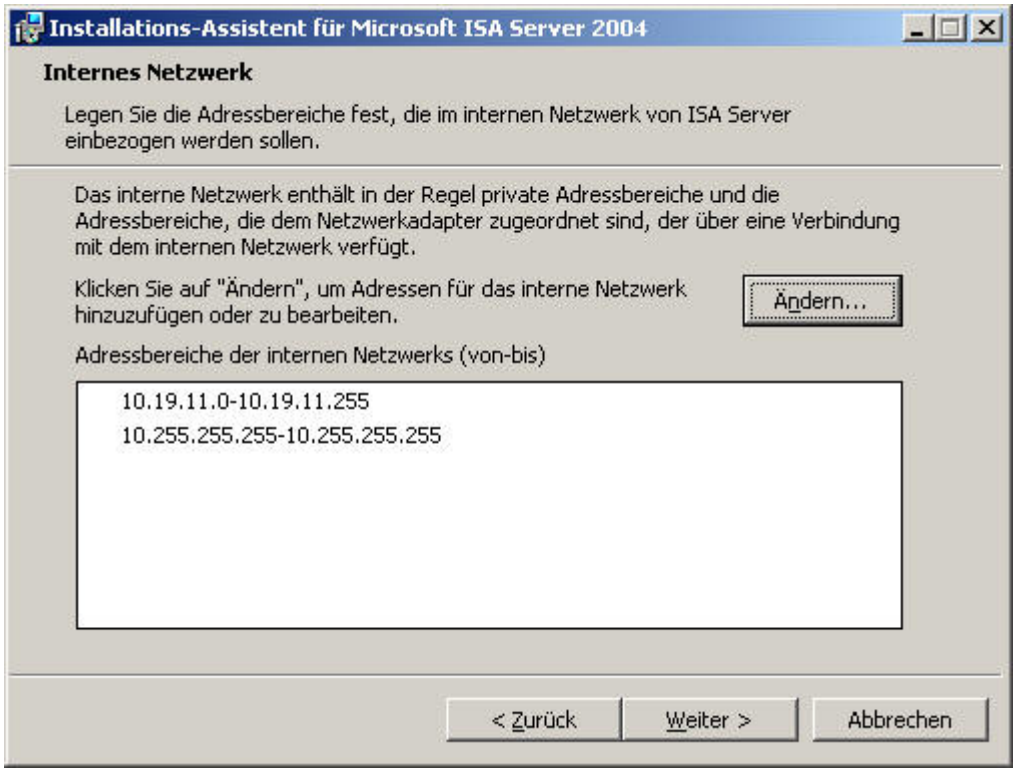
Als nächstes möchte der ISA Server wissen, welche IP-Adressen er als intern zu betrachten hat:



Durch "Hinzufügen" gelangt man hierher:

Hier können die IP-Bereiche entweder von Hand oder anhand der Routing-Tabelle hinzugefügt werden:





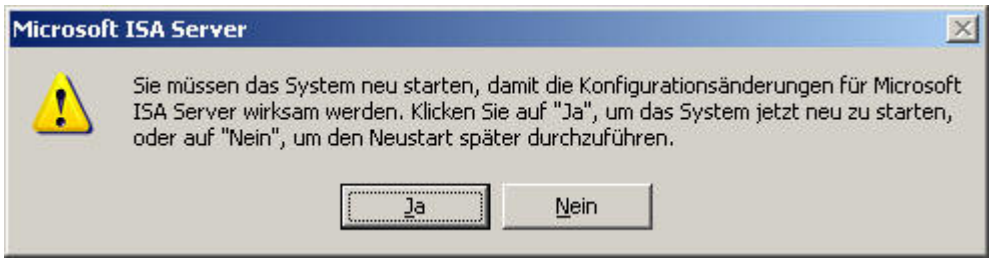
Als letztes wird man noch gefragt, ob auch ältere Firewallclients eine Verbindung zum ISA Server 2004 aufbauen können:

Hintergrund der Frage ist folgender: Mit dem ISA Server 2004 verwendet der ISA Server eine verschlüsselte Verbindung zum Firewallclient. Damit kommen natürlich ältere Firewallclients nicht zurecht und könnten keine Verbindung mehr aufbauen. Zwecks Abwärtskompatibilität kann auf die Verschlüsselung verzichtet werden.

Bevor es dann wirklich mit der Installation losgeht, kommt noch folgende Information:

Nach wenigen Minuten ist die Installation fertig gestellt:

In manchen Fällen ist ein anschließender Neustart des Servers notwendig.



Nun ist es Zeit, einen ersten Blick auf die neue Managementkonsole zu werfen:

Wer den ISA Server 2000 kennt wird sich fragen, wo denn die Abfrage nach dem Betriebsmode geblieben ist. Der ISA Server 2000 kannte ja die drei Betriebsmodi Firewallmodus, Cachemodus und Integrierter Modus. Ein Wechsel konnte nur durch Neuinstallation durchgeführt werden. Diese Abfrage und Einschränkung ist beim ISA Server 2004 weggefallen. Weitere Infos dazu im Artikel Cachemodus.

Aktivierung der Webcachefunktion beim ISA Server 2004

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Der ISA Server 2004 kann sämtlichen aus- und eingehenden Webverkehr für die Protokolle HTTP und FTP zwischenspeichern (=cachen). Wenn von internen Clients angeforderte externe Webseiten gespeichert werden spricht man vom Forward-Caching. Das Cachen der Seiten kann die Performance drastisch steigern. Der Flaschenhals beim Internetzugang ist heute nach wie vor die Bandbreite der Anbindung an den ISP. Interne Netzwerke haben heute fast überall mindestens 100MBit/s zur Verfügung, die Internetanbindung beträgt in kleinen und mittleren Unternehmen meist entweder 2 MBit/s synchron oder eine DSL Variante mit z.B. 3072/384kBit/s. Neben den Geschwindigkeitsvorteilen kann auch eine Kostenersparnis erreicht werden, sofern nicht sowieso eine feste Pauschale vereinbart wurde. Je langsamer und teurer die Internetanbindung desto lohnender erweist sich das Cachen.

Wie funktioniert nun das Caching?

Nehmen wir an, für die beiden Firewalladministratoren eines Unternehmens Michael und Manfred existiert eine Firewallrichtlinie, die ihnen das Surfen im Web erlaubt (HTTP zugelassen). Michael öffnet seinen Webbrowser und besucht die Webseite www.msisafaq.de und sieht sich dort einige Anleitungen an. Die Webseiten und die dazugehörenden Bilder werden vom ISA Server beim Zielwebserver im Auftrag von Michaels Client angefordert und im Cache des ISA Servers gespeichert (und natürlich sofort an Michaels Webbrowser gesendet). Michael erzählt Manfred davon und dieser besucht von seinem eigenen PC aus ebenfalls diese Webseite. Manfreds Webbrowser teilt dem ISA Server mit, welche Seite er angezeigt bekommen möchte. Der ISA schaut schnell in seinem Cache nach, ob er nicht schon auf der gewünschten Seite war. In diesem Beispiel ist das ja der Fall und der ISA prüft nur noch, ob es inzwischen eine aktuellere Seite am Zielwebserver gibt. Ist das der Fall, holt er die neuere Version und leitet sie an Manfreds Webbrowser weiter. Ist keine neue Version verfügbar, kann er Manfred die Seiten aus dem lokalen Cache zur Verfügung stellen. Dass das natürlich wesentlich schneller geht als wenn extra für Manfred die Seiten erneut komplett herunter geladen werden müssen sollte einleuchtend sein. Neben dem dadurch erzielten Geschwindigkeitsvorteil kann zusätzlich noch (kostbare) Bandbreite und je nach Tarif auch Volumenkosten eingespart werden. Je mehr Benutzer die selben Webseiten aufrufen desto größer der Vorteil.

Der ISA Server nutzt zwei Speichermedien für die gecachten Daten. Zuerst werden die Daten im RAM des Servers zwischengespeichert. Wenn der zur Verfügung stehende Platz erschöpft ist werden die Inhalte in ein Cachefile auf einer lokalen Festplatte geschrieben. Daher kann durch hinzufügen von RAM (und/oder einer Konfigurationsänderung) die Cachleistung erhöht werden.

Ergänzend dazu kann der ISA Server für so genannte "Inhaltdownloadaufträge" konfiguriert werden. Dadurch kann der ISA Server selbstständig zu einem vordefinierten Zeitplan

bestimmte (Teile von) Webseiten in seinen lokalen Cache laden, um sie zu einem späteren Zeitpunkt den Benutzern schneller zur Verfügung zu stellen. Der Download kann zum Beispiel nachts oder außerhalb der üblichen Geschäftszeiten erfolgen, um die weniger benutze Bandbreite auszunutzen, die ja tagsüber für wichtigere Dinge benutzt werden sollte. Wie ein solcher Inhaltdownloadauftrag konfiguriert wird, ist in einem eigenen Artikel beschrieben.

Wie eingangs erwähnt kann, der ISA neben dem gerade beschriebenen Forward Caching auch gerade entgegengesetzt cachen. Man spricht dann vom Reverse Caching. Was ist hier der Unterschied und wann wird was benötigt?

Ihr Unternehmen setzt den ISA Server ein um z.B. einen internen Webserver mit der Firmenwebseite zu veröffentlichen. Dazu wurde eine entsprechende Firewallrichtlinie erstellt. Wird nun diese Webseite von außen aufgerufen, klinkt sich wiederum der ISA zwischen die Anfrage und ruft stellvertretend für den Webclient (als Proxy) die Seiten auf. Dabei lädt er sie natürlich wieder in seinen lokalen Cache. Wird die Seite zu einem späteren Zeitpunkt erneut abgerufen, kann der ISA - nach kurzer Aktualitätsprüfung - die Seiten aus seinem lokalen Cache bereitstellen. In diesem Szenario wird nicht zwingend Bandbreite gespart. Dafür wird der Webserver entlastet, da er nicht mehr jede Anfrage selber beantworten muss.

Denkbar ist auch, den ISA Server als Webproxy innerhalb eines Unternehmens als Cacheengine vor einem stark-besuchten Intranetserver aufzubauen. Nur, um mal eine etwas größere artfremde Idee zu nennen....

Unmittelbar nach der Installation des ISA Server 2004 ist die Cachefunktionalität nicht aktiviert.

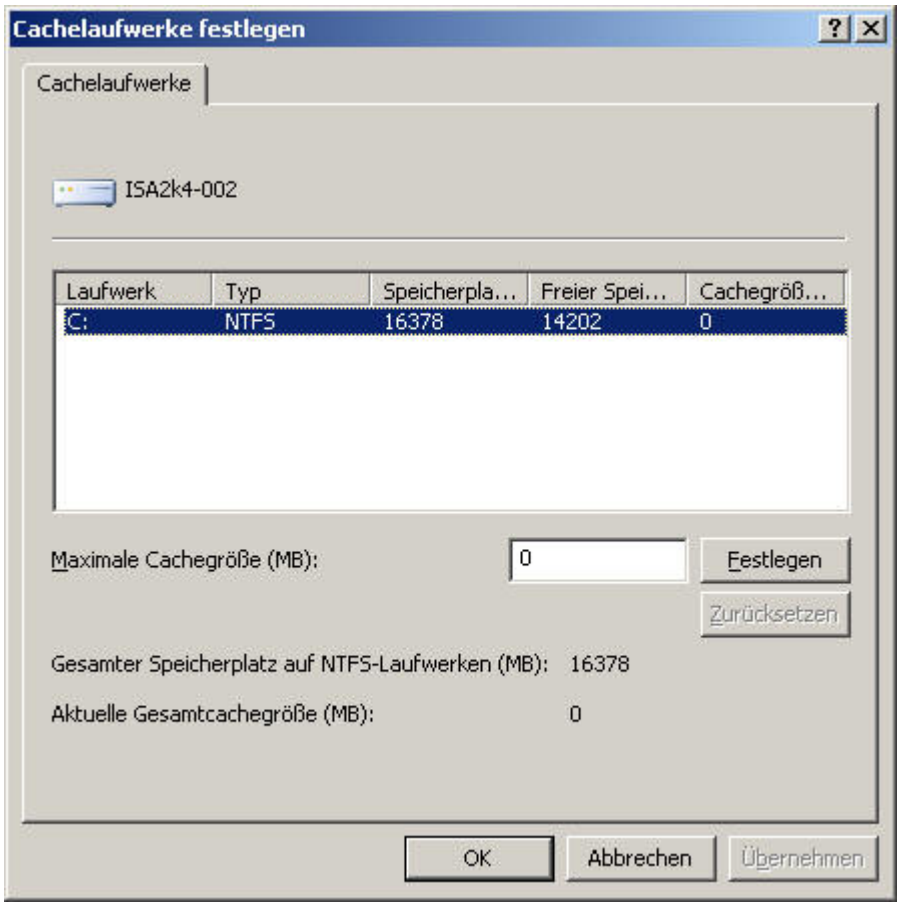
Dies muss bei Bedarf nachgeholt werden (was ich für die meisten Anwendungsfälle empfehle).

Als erstes muss ein Cachelaufwerk definiert werden.

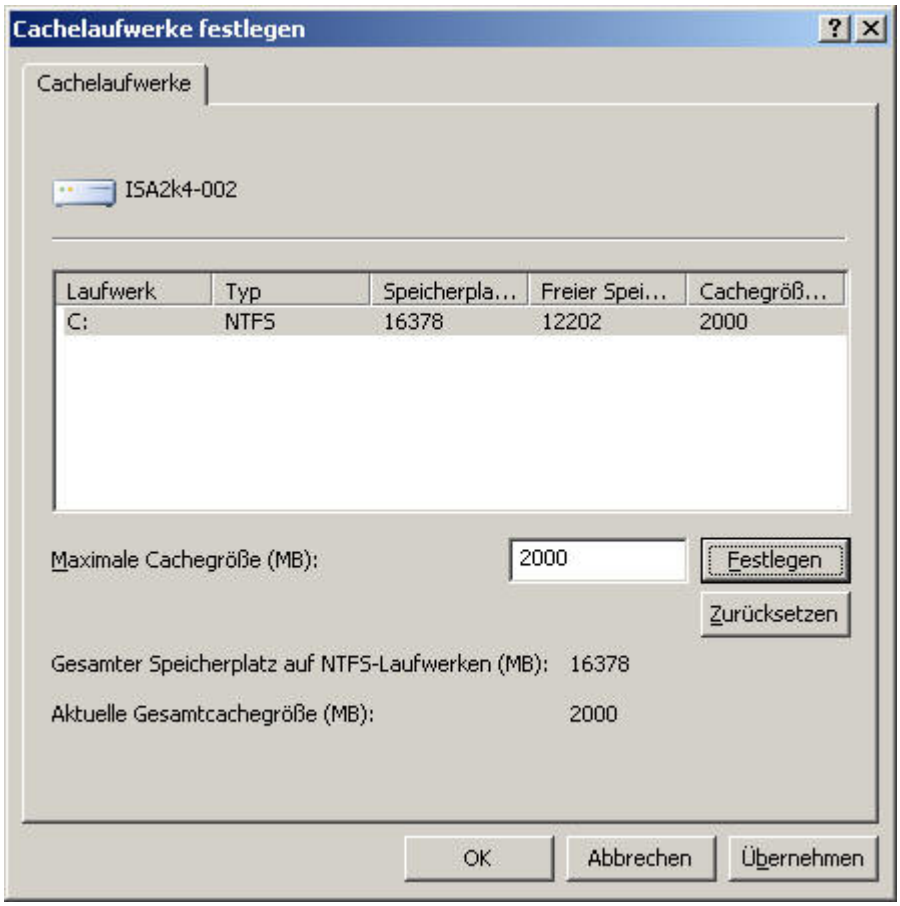
Dazu kann man den Aufgabenbereich...

...oder das Kontextmenü verwenden:...

Anschließend erhält man die Laufwerksdefinitionsbox:



Je nach Anzahl der vorhandenen Festplatten/Volumes werden natürlich mehrere Laufwerke angeboten als im oberen Beispiel. Es empfiehlt sich aus Performancegründen, das Cachefile auf eine separate schnelle Festplatte zu legen. Die Größe ist individuell und ich möchte hier keine Regelempfehlung machen.



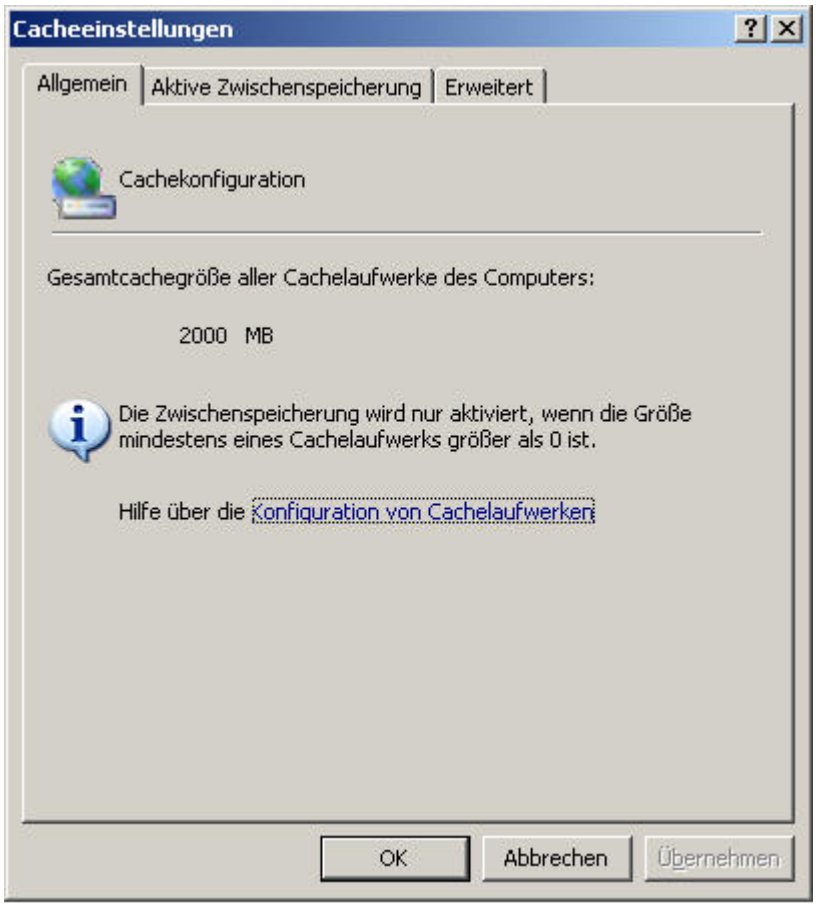
Im obigen Beispiel wurde ein Cachefile von 2000 MB festgelegt.

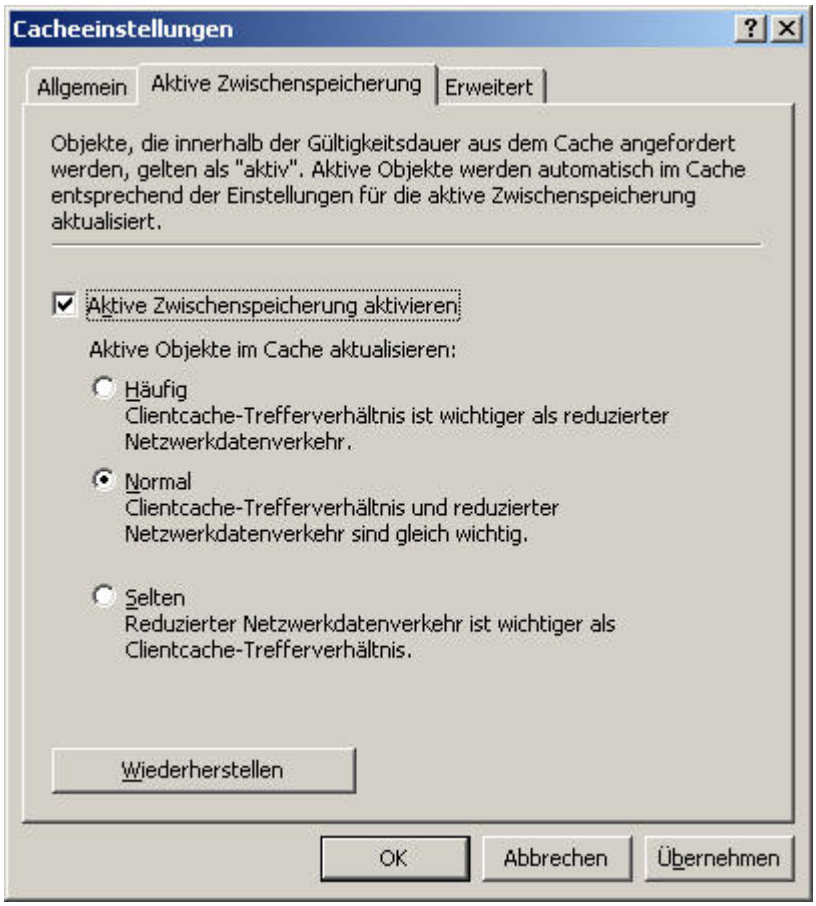
Natürlich müssen die Einstellungsänderungen wie beim ISA Server 2004 üblich übernommen werden:

Da anschließend auch der Firewalldienst neu gestartet werden muss wird der Administrator darauf hingewiesen.

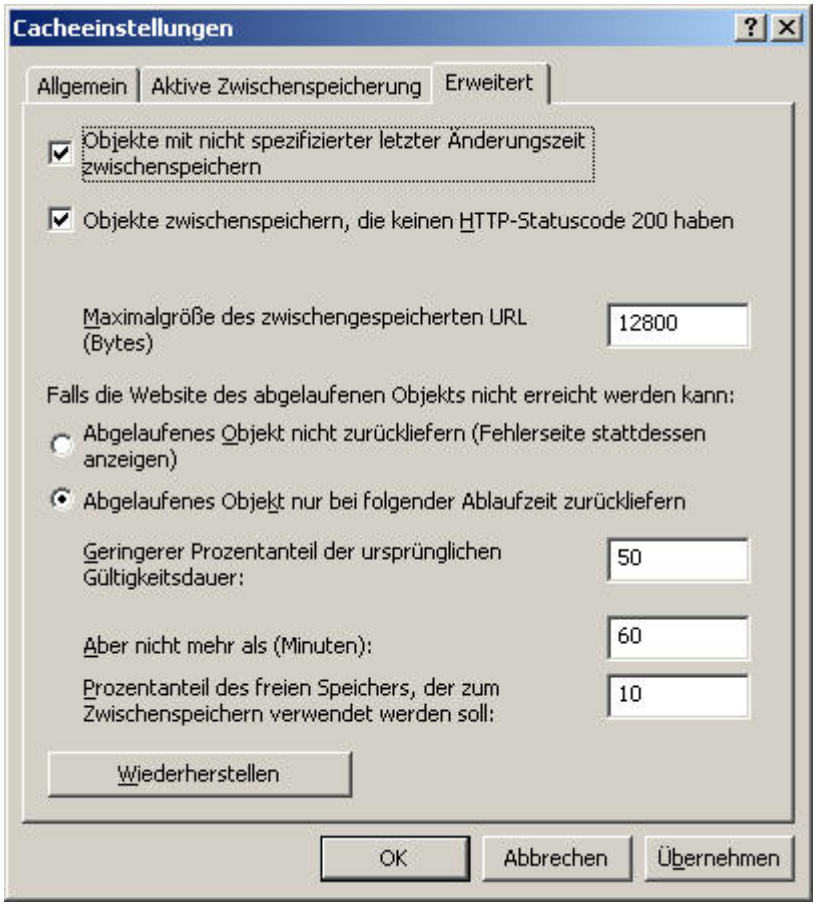
Sobald der Diensteneustart erfolgt ist, werden alle Webanfragen zwischengespeichert.

Anschließend kann man in den Eigenschaften der Cacheeinstellungen noch einiges konfigurieren:





Wenn die "Aktive Zwischenspeicherung" aktiviert ist lädt der ISA Server selbstständig Objekte aus dem Internet nach, die häufig angefordert werden. Diese Option empfiehlt sich nur dann zu aktivieren, wenn man keinen Zeit- oder Volumenabhängigen Tarif verwendet.



Ähnlich wie beim ISA Server 2000 können einige Zwischenspeicherungsoptionen gesetzt werden. Die interessanteste Einstellung dabei ist der "Prozentanteil des freien Speichers, der zum Zwischenspeichern verwendet werden soll". Die Standardeinstellung ist 10%. Soll der ISA (auch) als Cacheengine verwendet werden und verfügt er über genügend RAM kann der Wert erfahrungsgemäß bis auf 80 oder 90% erhöht werden. D.h. dass wesentlich mehr RAM für den schnellen Zwischenspeicher verwendet wird. Hierduch wird eine deutlich gesteigerte Performance erreicht.

Erkennung von Eindringversuchen und DNS-Angriffen aktivieren

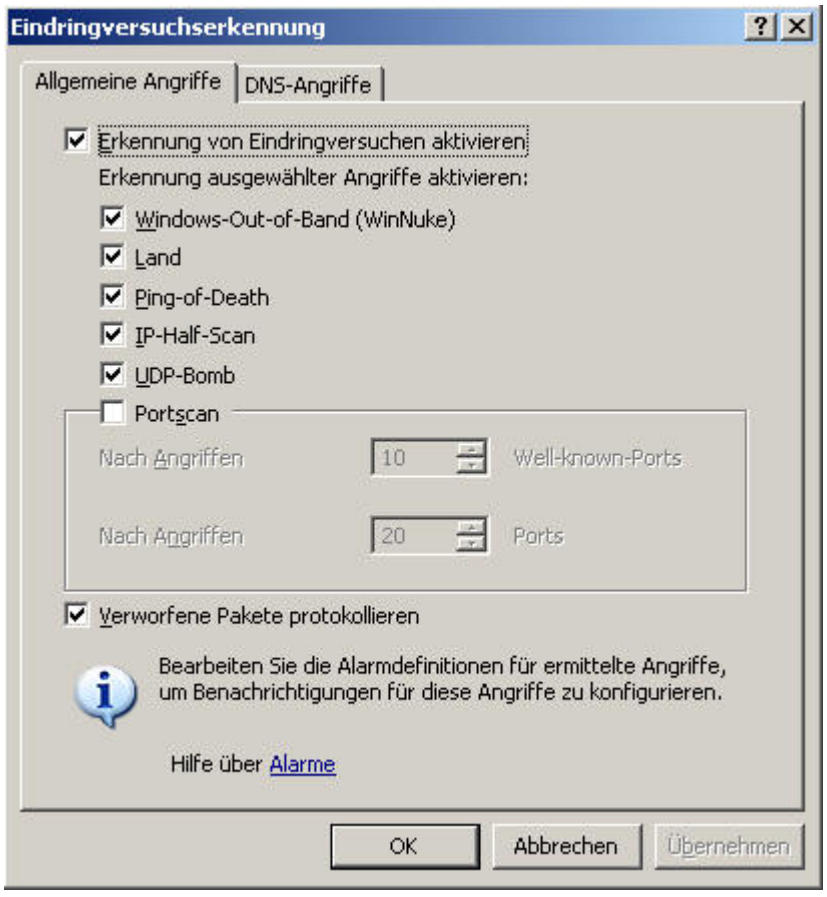
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Der ISA Server bietet neben den Firewall- und Proxyfunktionen auch eine Eindringversuchserkennung. Microsoft hat diesen Bestandteil von ISS (www.iss.net/isaserver) lizenziert; ISS bietet darüber hinaus für den ISA weitere Komponenten an, die mehr Erkennungsmuster für Angriffsversuche mitbringen. Sobald die Eindringversuchserkennung aktiviert ist, erkennt der ISA Angriffsversuche und kann darauf reagieren. Es besteht die Möglichkeit, das Ereignis nur im Ereignisprotokoll zu vermerken, z.B. dem Administrator eine E-Mail zu senden, Dienste herunter zu fahren oder Anwendungen auszuführen.

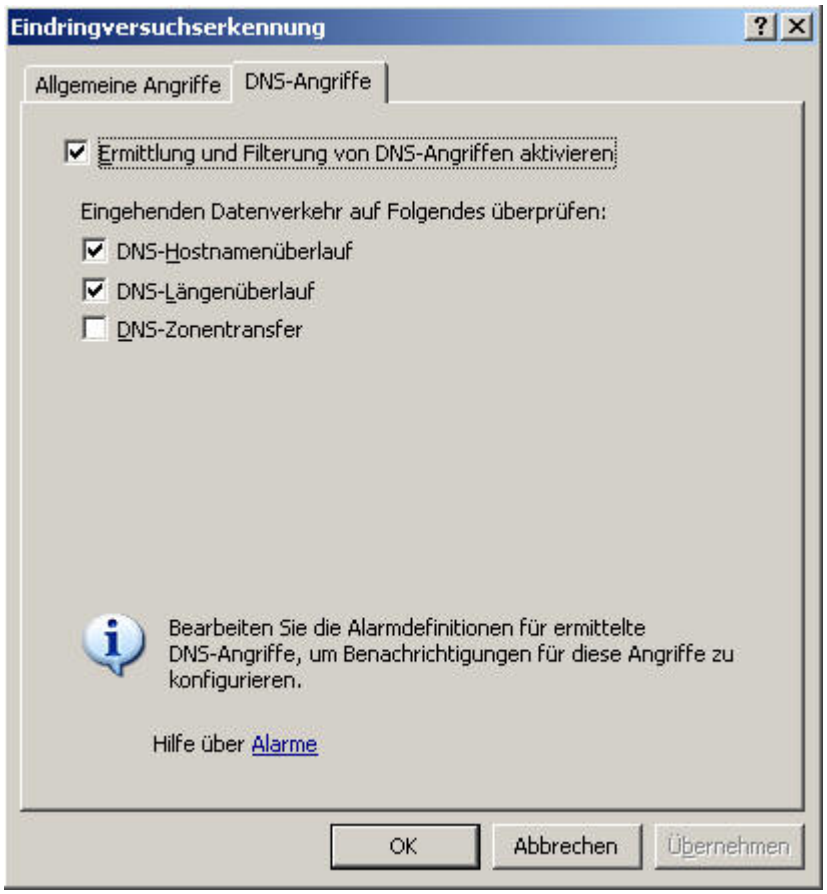
Aktiviert wird die Eindringversuchserkennung in der allgemeinen ISA Server Verwaltung (ISA Managementkonsole -> Allgemein):

Erkennung von Eindringversuchen und DNS-Angriffen aktivieren



- **Windows-Out-of-Band (WinNuke)**
  Tritt auf, wenn Angreifer einen Out-of-Band-Angriff oder Denial of Service (DoS)-Angriff gegen einen Computer ausführen. Ein DoS-Angriff ist ein Versuch, einen Computer oder ein Netzwerk lahm zu legen. Dieser Angriff kann dazu führen, dass der Computer nicht mehr antwortet oder die Netzwerkverbindung verliert. Dazu wird ein Sicherheitsloch in Windows-Betriebssystemen (für das ein Patch seit Windows NT 4.0 ServicePack 4 existiert!) ausgenutzt und an Port 139 ein leeres IP-Paket gesendet, welches das TCP Flag Urgent gesetzt hat.
- **Land**
  Damit bezeichnet man die Methode, wenn Eindringlinge eine TCP-Verbindung mit einer gefälschten Quell-IP-Adresse und Portnummer aufbauen, welche mit der Ziel-IP-Adresse und Portnummer übereinstimmt. Spoofing bezieht sich auf das Überlisten eines Computers, um Informationen zu erhalten, welche unberechtigten Zugriffe mit Hilfe einer falschen IP-Adresse erlauben. Ein Land-Angriff kann bewirken, dass Computer nicht mehr reagieren und so auch für berechtigte Benutzer nicht mehr zur Verfügung stehen.
- **Ping-of-Death**
  Mit Ping-of-Death-Angriffen wird versucht, einen Computer außer Kraft zu setzen, in dem ICMP Echo Request-Paketen große Datenmengen hinzugefügt werden. Bei dieser Attacke sendet der Angreifer ICMP-Pakete mit einer Nutzdatengröße von mindestens 65.510 Byte. Diese werden fragmentiert zum Zielsystem übertragen und dort wieder zusammengesetzt. Inklusive des ping-Headers ergibt das ein IP-Paket, das größer ist als die maximal zulässige Größe von 65.536 Byte. Bei IP-Implementierungen, die einen solchen Overflow nicht abfangen, kommt es dann zum Systemabsturz
- **IP-Half-Scan**
  Treten auf, wenn Eindringlinge wiederholt versuchen, eine Verbindung zum Zielcomputer herzustellen und die TCP-Pakete bestimmte Flags enthalten. Die bestimmten Flags sind Sync = 1. Daraufhin sendet der Ziel Server die Flags Sync=1 und zusätzlich das ACK=1 Flag. Als nächstes müsste der Angreifer ein IP Paket senden das nur noch das Ack=1 Flag gesetzt hat, das tut er aber nicht (ein halber Port Scann also). Dieser Vorgang kann darauf hindeuten, dass nach offenen Ports gesucht wird.
- **UDP-Bomb**
  Tritt auf, wenn Eindringlinge versuchen, ein illegales UDP-Paket zu senden. Ein UDP-Paket, das aus illegalen Werten in bestimmten Feldern aufgebaut ist, bringt den Computer zum Absturz, sobald das Paket empfangen wird.
- **Port-Scan**
  Ein Port-Scan (All-Port-Scan) tritt auf, wenn Angreifende versuchen, Zugriff auf mehr als die vorkonfigurierte Anzahl der Ports zu erhalten. Der Administrator definiert einen Portbereich (siehe Bild), wodurch die Anzahl der Porte festgelegt wird, die für den Zugriff verfügbar sind. Eindringlinge verwenden das Scannen von Ports, um offene Ports eines Computers zu finden. Offene Ports stellen einen Eingang in diese Computersysteme dar und dadurch kann versucht werden, einen Angriff über einen oder mehrere dieser Ports durchzuführen.

Neben der Eindringversuchserkennung auf IP-Paketfilterebene hat der ISA Server2004 auch einen DNS-Filter:



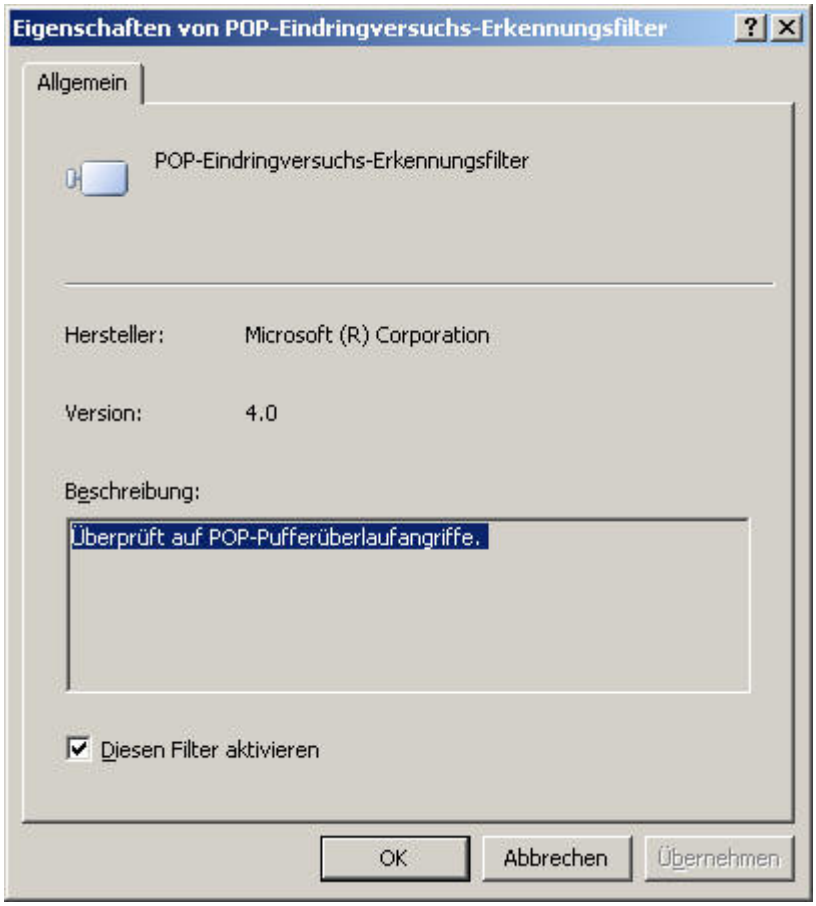
- **DNS-Hostnamenüberlauf**
  Tritt ein, wenn eine Antwort eines DNS-Servers für einen Hostnamen eine bestimmte feste Länge überschreitet. Dieser Angriff kann bei fehlerhaft geschriebenen Anwendungen, welche die Länge des Hostnamens nicht überprüfen bewirken, dass die internen Puffer überlaufen. sobald der Hostname kopiert wird. Dieser Angriff kann es einem Angreifer ermöglichen, beliebige Befehle auf dem angegriffenen Computer auszuführen.
- **DNS-Längenüberlauf**
  Tritt ein, wenn eine IP-Adresse ein Feld enthält, dessen Wert größer als 4 Byte ist. Dieser Angriff kann bei fehlerhaft geschriebenen Anwendungen, die DNS-Suchen durchführen einen internen Pufferüberlauf bewirken. Dieser Angriff kann es einem Angreifer ermöglichen, beliebige Befehle auf dem angegriffenen Computer auszuführen.
- **DNS-Zonentransfer**
  Legt fest, dass der Filter prüfen soll, ob Eindringversuche vom Typ DNS-Zonentransfer stattgefunden haben. Ein DNS-Zonentransfer tritt auf, wenn ein Clientsystem eine DNS-Clientanwendung für die Übertragung von Zonen von einem internen DNS-Server verwendet.

Ergänzend zu den oben vorgestellten Eindringversuchserkennungsmöglichkeiten stellt der ISA Server 2004 auch einen POP-Eindringungs-Erkennungsfilter zur Verfügung.

Der POP-Eindringungs-Erkennungsfilter fängt für das interne Netzwerk bestimmten POP-Datenverkehr zum Zweck der Analyse ab. Der Anwendungsfilter überprüft insbesondere POP-Pufferüberlaufangriffe. Ein POP-Pufferüberlaufangriff tritt dann auf, wenn ein

Remoteangreifer versucht, als Superuser eines POP-Servers Zugriff zu erhalten, indem ein interner Puffer auf dem Server zum Überlaufen gebracht wird.

Der POP-Eindringungs-Erkennungsfilter bietet keine Konfigurationsmöglichkeit und befindet sich - im Gegensatz zu den oberen beiden - bei den Anwendungsfiltern.



Man könnte ggfs. noch den SMTP-Filter in den Bereich Eindringversuchserkennung aufnehmen, da dieser Anwendungsfilter SMTP-Kommandos abweisen sowie den Mailverkehr überwachen kann.

ISA Server 2004 als reinen Webproxyserver konfigurieren

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Bei der Installation des ISA Server 2000 musste man sich entscheiden, welchen Betriebsmode man verwenden möchte. Eine Änderung konnte nur durch Neuinstallation erfolgen.

Wollte man den ISA Server nur als Webcacheserver verwenden (um seine Stärken im Caching auszunutzen) und auf die Firewallfunktionalitäten verzichten, musste man den Cachemodus auswählen. In der Regel befindet sich dabei eine weitere Firewall an der äußeren Schnittstelle des Netzwerks zur Verbindung des Firmennetzwerks mit dem Internet. In diesem Szenario mit einem Adapter fungiert ISA Server normalerweise als Cacheserver, auf dem die Inhalte aus dem Internet zwischengespeichert und für Clients im Firmennetzwerk bereitgestellt werden.

Wer den ISA Server 2004 schon mal installiert hat, wird feststellen, dass es keine Abfrage mehr gibt, in welchem Modus er installiert werden soll. Soll das heißen, dass der 2004er das nicht mehr unterstützt?

Natürlich kann der Internet Security and Acceleration Server 2004 jederzeit auch nur als Cacheserver verwendet werden (deswegen ja das "Acceleration" in seinem Namen). Der Cachemodus wird durch die mitgelieferte Netzwerkvorlage "Einzelner Netzwerkadapter" vorbereitet. Das Netzwerkmodell beim 2004er ist völlig anders und wesentlich flexibler als das des 2000er Servers. Für die häufigsten Netzwerklayouts gibt es Vorlagen, die dem ISA Administrator die Grundeinrichtung erleichtern.

Bei Anwendung der Einzelnetzwerkadapter-Netzwerkvorlage wird das interne Netzwerk so konfiguriert, dass es alle IP-Adressen enthält. Die Firewallrichtlinie "Standardwebproxy- und -zwischenspeicherkonfiguration verwenden" wird angewendet. Diese Richtlinie gestattet Webproxyclients den Zugriff auf Webinhalte im Internet und erhöht die Webleistung durch Zwischenspeicherung. Es werden jedoch keine Regeln erstellt.

Eine der grundlegenden Funktionen von ISA Server besteht darin, mehrere Netzwerke miteinander verbinden zu können. Wenn ISA Server auf einem Computer mit einem Adapter installiert ist, wird allerdings nur ein Netzwerk erkannt: das interne Netzwerk. Das interne Netzwerk umfasst alle IP-Adressen mit Ausnahme der folgenden: 0.0.0.0, 255.255.255.255 und den Adressbereich 127.0.0.0–127.255.255.255. Bei der Einrichtung des Netzwerkes müssen Sie die Adressen festlegen, die im internen Netzwerk enthalten sein sollen. Wenn Sie ISA Server auf einem Computer mit nur einem Netzwerkadapter installieren, muss sichergestellt werden, dass alle Adressen (mit Ausnahme

von 0.0.0.0, 255.255.255.255 und des Adressbereichs 127.0.0.0–127.255.255.255) in das interne Netzwerk aufgenommen werden.

In diesem Szenario wird die standardmäßige Firewallrichtlinie von Ihnen dahingehend geändert, dass internen Clients der Zugriff auf das Internet gestattet wird. Obwohl hierbei gilt, dass alle IP-Adressen zum selben internen Netzwerk gehören, kann ISA Server aufgrund der Standardregel Alle verwerfen unter Umständen auch Webdatenverkehr verweigern. Sie müssen daher eine Regel erstellen, die die Durchleitung des Datenverkehrs zwischen den Netzwerken zulässt.

Um dieses Cachingszenario zu ermöglichen, müssen Sie eine Zugriffsregel erstellen, die allen Clients die Verwendung von HTTP und möglicherweise auch HTTPS und FTP gestattet. Da das interne Netzwerks laut eindeutiger Definition alle Adressen umfasst, muss das Quell- und das Zielnetzwerk für diese Regel jeweils das interne Netzwerk sein.

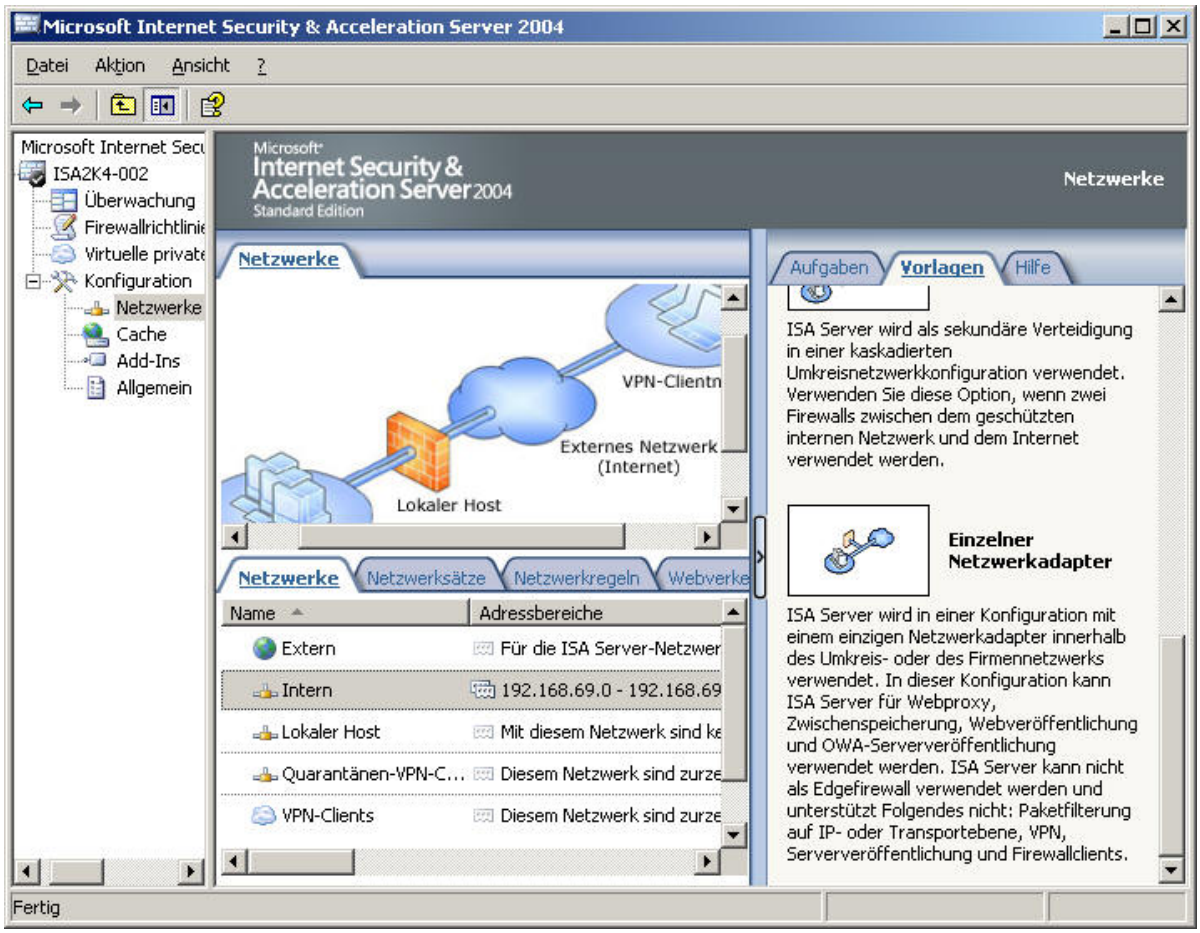
Sie können ISA Server auf einem Computer mit einem einzelnen Netzwerkadapter als Reversewebproxy einsetzen und Szenarien für die Webveröffentlichung und Outlook Web Access-Veröffentlichung ermöglichen.

Bei der Installation von ISA Server auf einem Computer mit einem einzelnen Adapter können die folgenden ISA Server-Funktionen nicht verwendet werden:

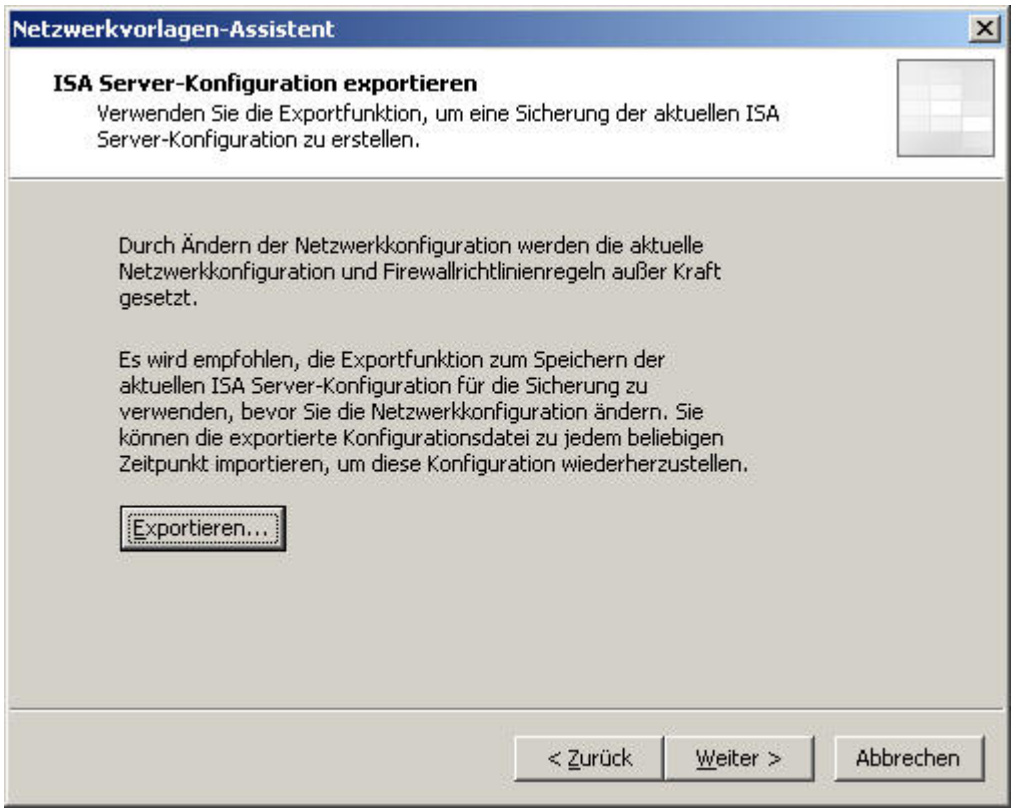
- Firewallclients
- Virtuelle private Netzwerke
- IP-Paketfilterung
- Firewallrichtlinie für mehrere Netzwerke
- Serververöffentlichung
- Filterung auf Anwendungsebene
- Die folgenden Protokolle werden unterstützt: HTTP, HTTPS und FTP über HTTP.

Daraus ergibt sich eine eingeschränkte Sicherheitsfunktion von ISA Server in Ihrem Netzwerk.

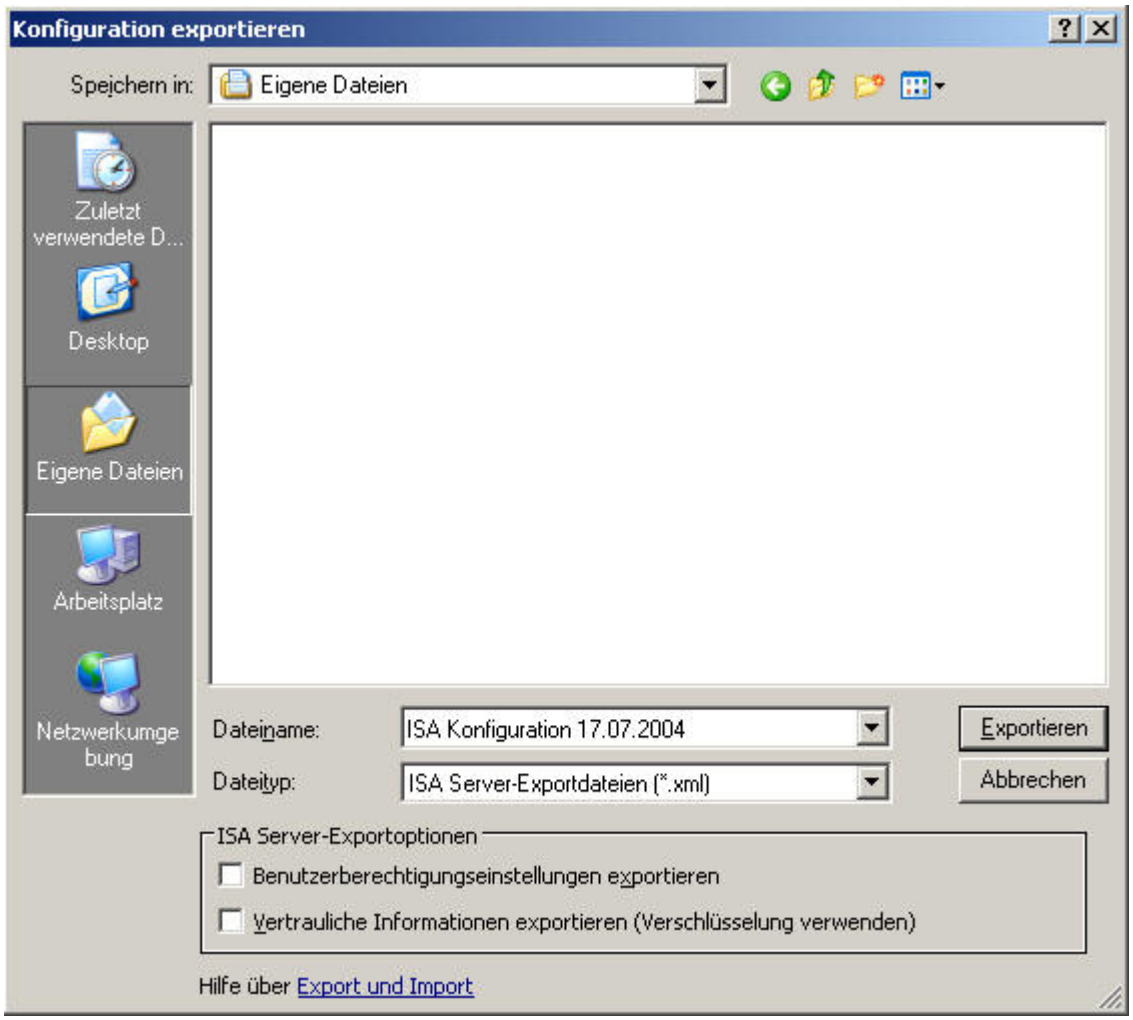
Um die Netzwerkvorlage einmalig einzurichten oder zu ändern gehen Sie in der ISA Managementkonsole auf den Knoten "Netzwerke" und wählen in der Taskbar rechts unter Vorlagen die "Einzelner Netzwerkadapter"-Vorlage aus.

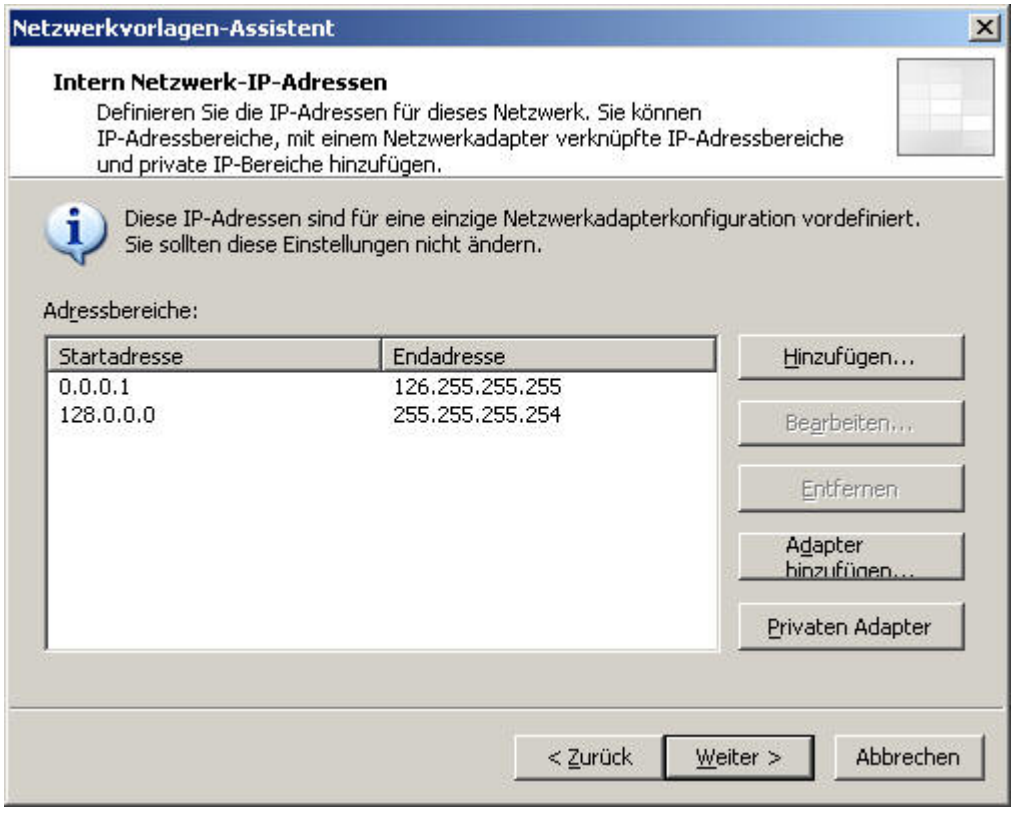


Wie nicht anders zu erwarten war, führt ein Assistent durch die notwendigen Konfigurationsschritte:



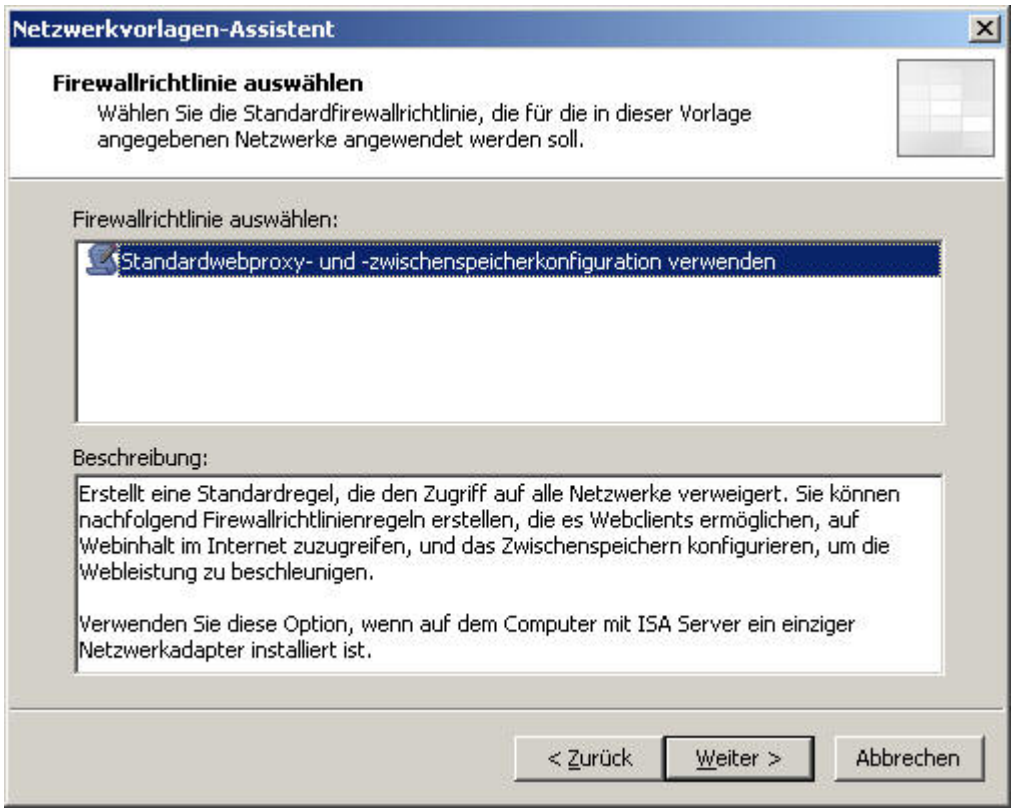
Egal, ob der ISA soeben frisch aufgesetzt wurde oder nicht, empfehle ich dringend, an dieser Stelle die aktuelle Konfiguration zu exportieren. Schade, dass Microsoft hier keine Zwangsexportfunktion eingebaut hat.


Konfiguration exportieren
Speichern in:
Eigene Dateien
Zuletzt verwendete D...
Desktop
Eigene Dateien
Arbeitsplatz
Netzwerkumgebung
Dateiname:
ISA Konfiguration 17.07.2004
Dateityp:
ISA Server-Exportdateien (*.xml)
Exportieren
Abbrechen
ISA Server-Exportoptionen
Benutzerberechtigungseinstellungen exportieren
Vertrauliche Informationen exportieren (Verschlüsselung verwenden)
Hilfe über Export und Import


Netzwerkvorlagen-Assistent
Intern Netzwerk-IP-Adressen
Definieren Sie die IP-Adressen für dieses Netzwerk. Sie können IP-Adressbereiche, mit einem Netzwerkadapter verknüpfte IP-Adressbereiche und private IP-Bereiche hinzufügen.
Diese IP-Adressen sind für eine einzige Netzwerkadapterkonfiguration vordefiniert. Sie sollten diese Einstellungen nicht ändern.
Adressbereiche:
Startadresse
Endadresse
0.0.0.1
126.255.255.255
128.0.0.0
255.255.255.254
Hinzufügen...
Bearbeiten...
Entfernen
Adapter hinzufügen...
Privaten Adapter
< Zurück
Weiter >
Abbrechen

Hier schlägt der Assistent vor, die im Eingangstext oben beschriebenen Adressbereiche zu verwenden.

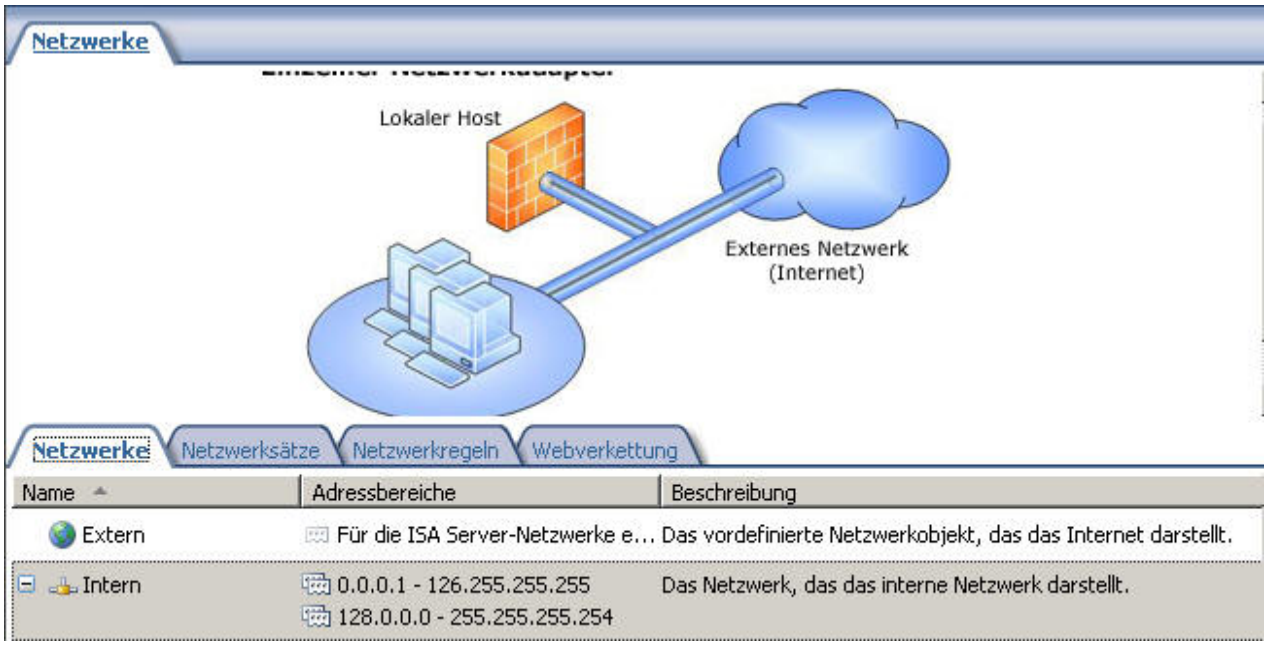
Anschließend richtet der ISA noch eine Defaultfirewallrichtlnie ein, die sicherstellt, dass sämtlicher Verkehr gesperrt wird. Nach Beendigung der Netzwerkkonfiguration müssen dann entsprechende Zulassungsregel erstellt werden.



Abschließend wieder die gewohnte Zusammenfassung:

Bevor die Änderung wirksam wird, muss wie gewohnt erst der "Übernehmen"-Knopf gedrückt werden:

Das Netzwerkmodell hat sich wie folgt geändert:



Firewallrichtlinie
R...
Name
Aktion
Protokolle
Von / Listener
Nach
Bedingung
L... Standardregel
Verweigern
Gesamter ...
Alle Netzwerke (und lokaler Host)
Alle Netzwer...
Alle Benutzer

Bestimmte WebSeiten nicht cachen

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

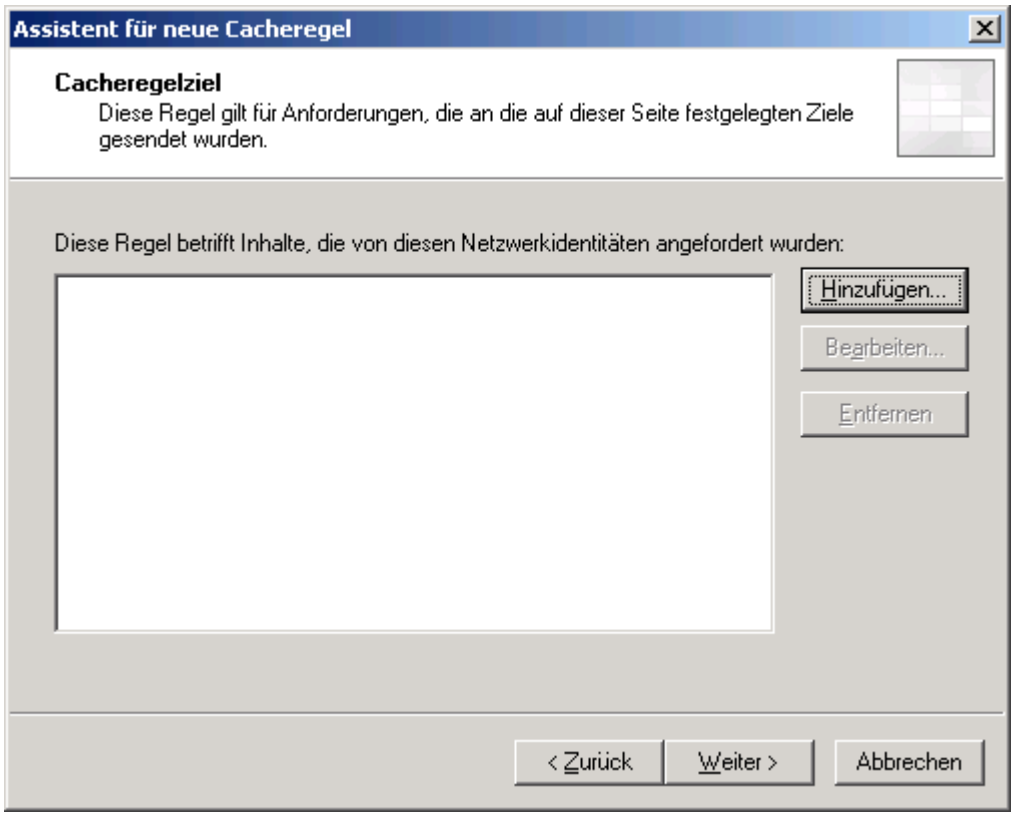
Grundsätzlich speichert der ISA Server alle extern abgerufenen Webseiten und ggfs. FTP-Downloads im Cache, sofern dieser eingerichtet wurde..

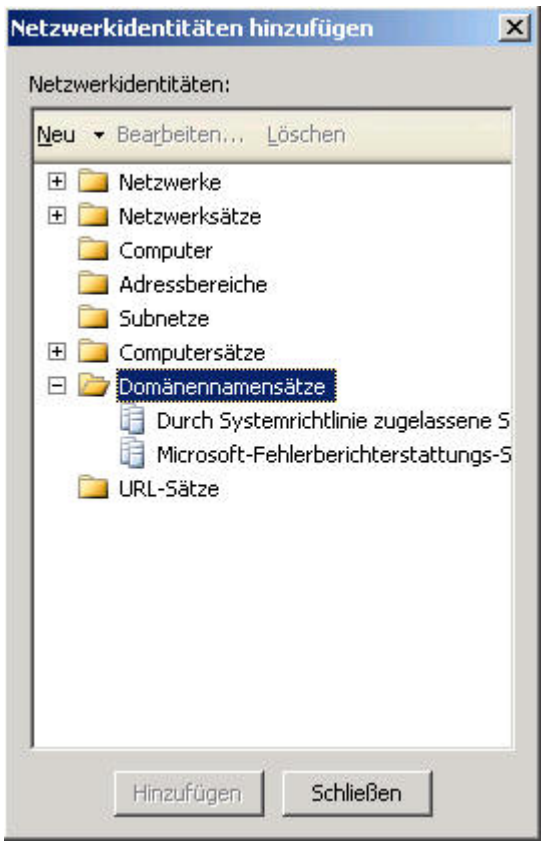
In einigen Situationen ist es notwendig, bestimmte externe Webseiten nicht zu cachen. Dies kann durch eine zusätzliche Cacheregel eingerichtet werden, was in diesem Artikel ausführlich beschrieben wird.

Im folgenden Beispiel wird eine Regel eingerichtet, die alle Anfragen an die Webseite www.msisafaq.de nicht zwischenspeichert.

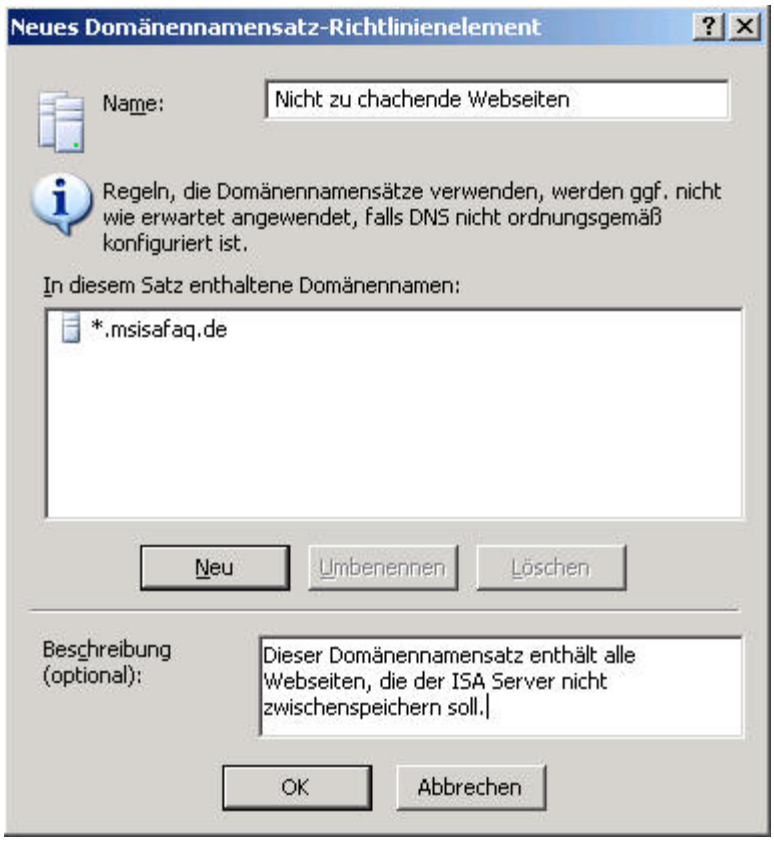
In der Management Konsole unter Konfiguration gibt es den Punkt "Cache". Dort findet man entweder im Kontextmenü oder im Aufgabenbereich die Möglichkeit, eine neue Cacheregel zu erstellen.

Hier sollte wie immer ein beschreibender Name eingegeben werden.

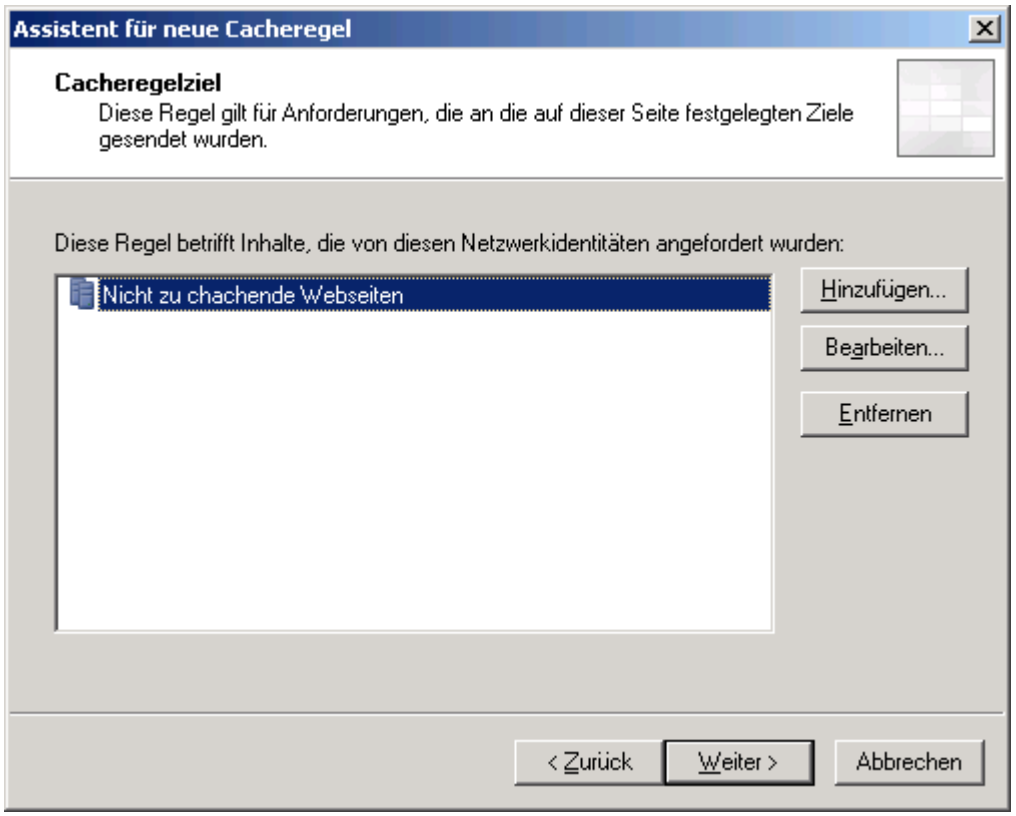




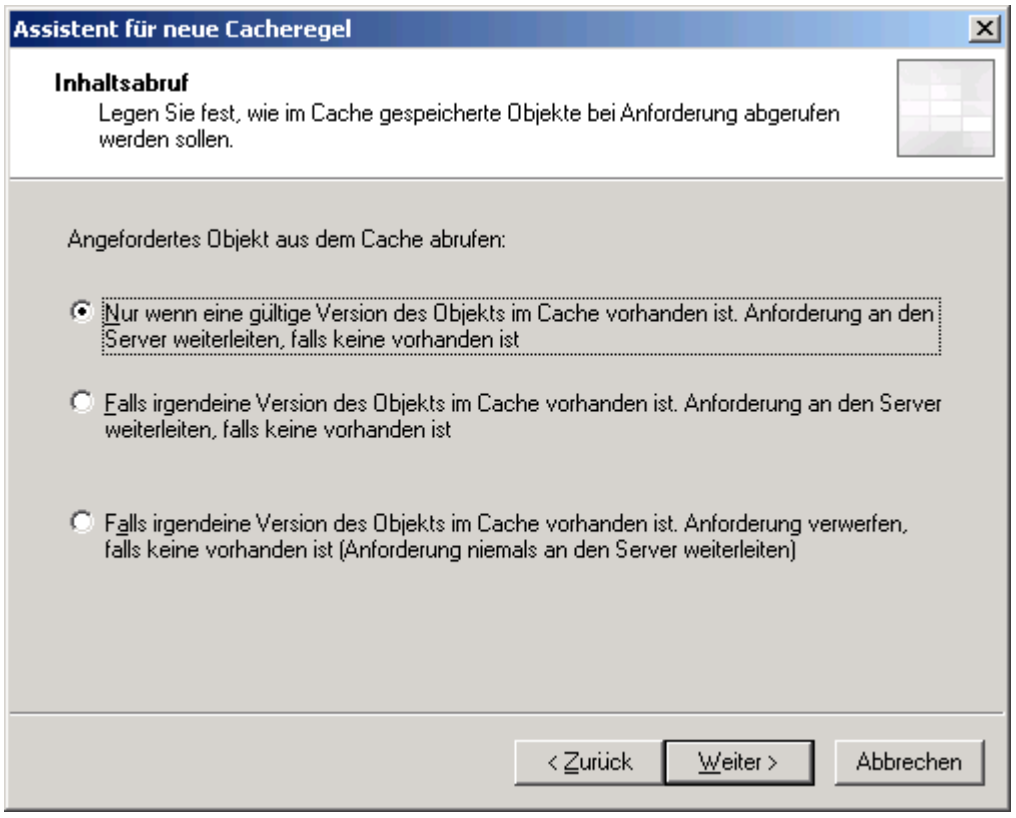
Sofern nicht bereits zu einem früheren Zeitpunkt erledigt, muss hier nun ein neuer Domänennamensatz erstellt werden.

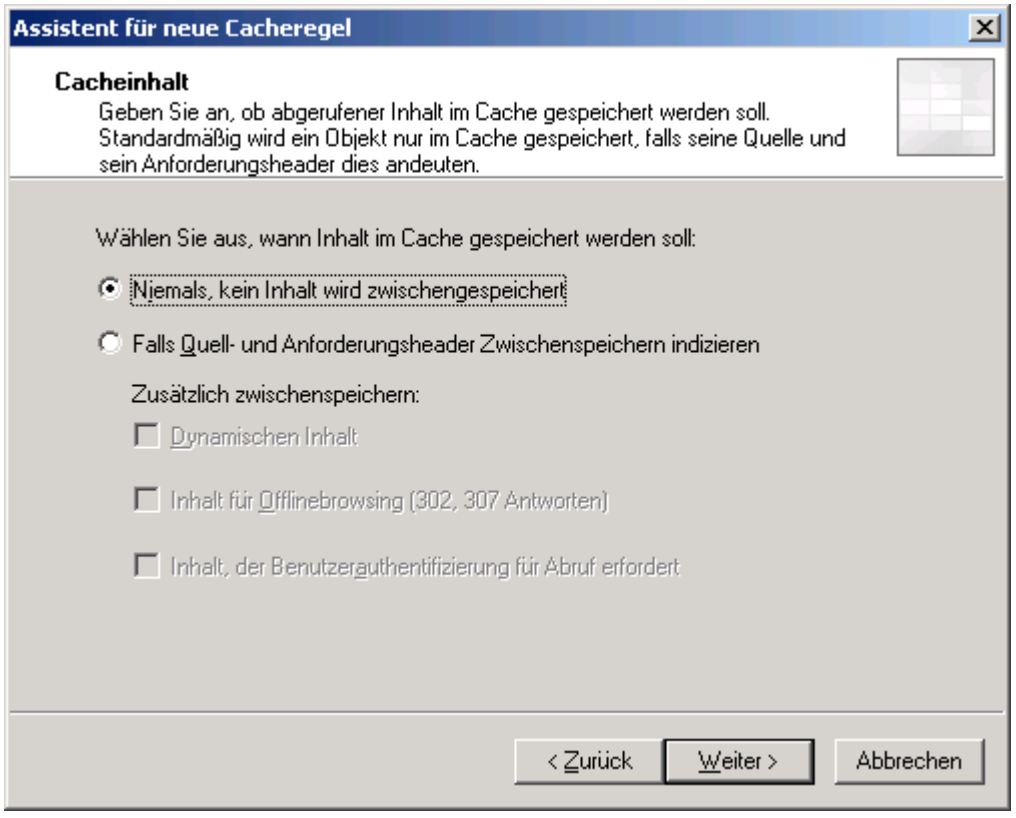


Administratoren, die sich mit dem ISA Server 2000 auskennen werden die neuen Funktionen der 2004er Version sehr schätzen. Mussten früher alle Elemente, die für eine Regel notwendig waren, im Vorfeld definiert werden, kann das nun beim Erstellen einer Regel in einem Schritt durchgeführt werden.



Die folgende Assistentenseite kann ohne Änderung übernommen werden:

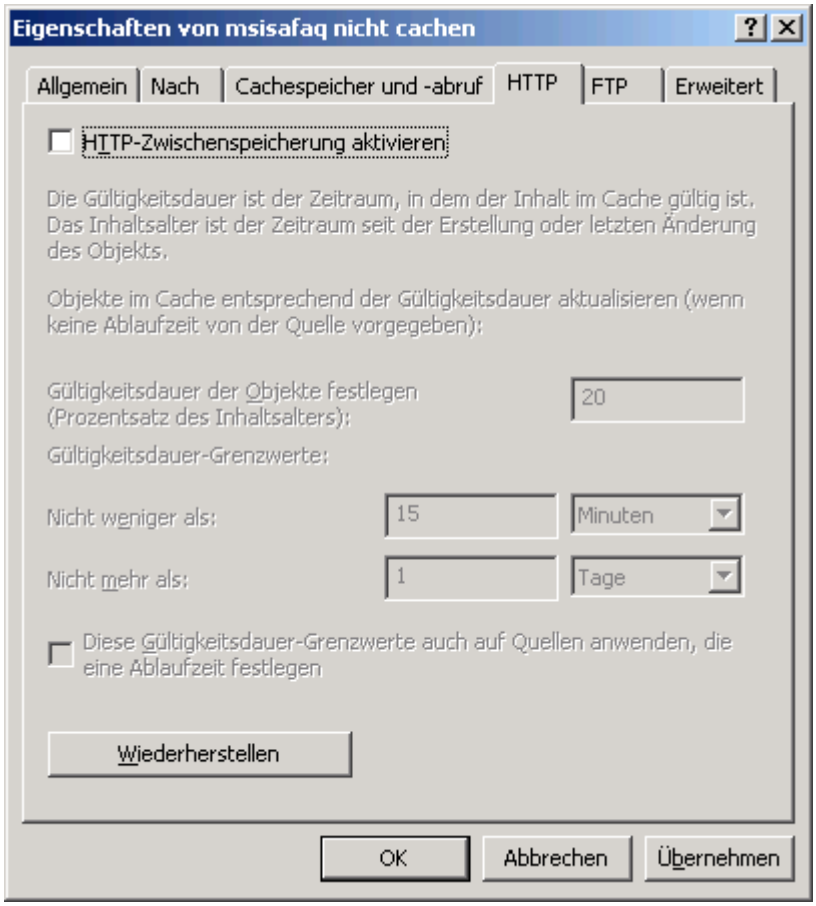




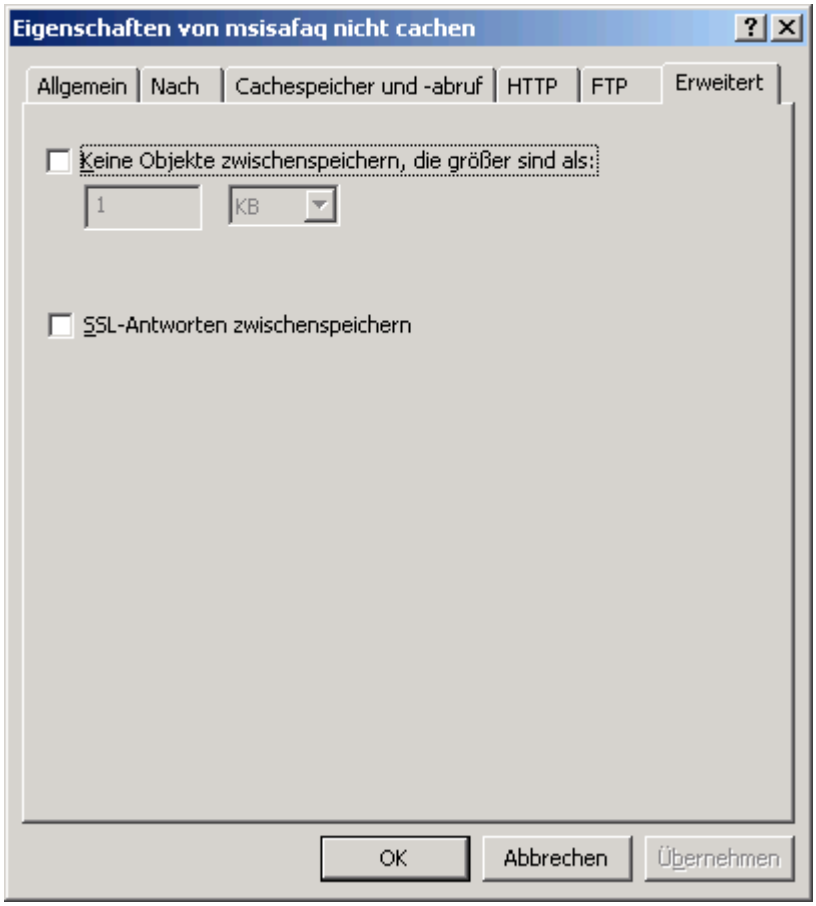
Hier wird festgelegt, dass kein Inhalt zwischengespeichert werden soll.

Abschließend die obligatorische Zusammenfassungsseite, die man als Dokumentation weiterverwenden könnte.

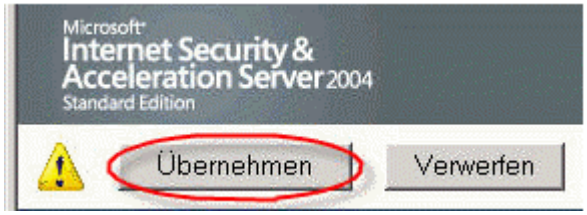
Zum Schluss sollte man in den Eigenschaften der neu erstellten Regel noch folgende Änderungen durchführen:


Eigenschaften von msisafaq nicht cachen
Allgemein
Nach
Cachespeicher und -abruf
HTTP
FTP
Erweitert
HTTP-Zwischenspeicherung aktivieren
Die Gültigkeitsdauer ist der Zeitraum, in dem der Inhalt im Cache gültig ist. Das Inhaltsalter ist der Zeitraum seit der Erstellung oder letzten Änderung des Objekts.
Objekte im Cache entsprechend der Gültigkeitsdauer aktualisieren (wenn keine Ablaufzeit von der Quelle vorgegeben):
Gültigkeitsdauer der Objekte festlegen (Prozentsatz des Inhaltsalters):
20
Gültigkeitsdauer-Grenzwerte:
Nicht weniger als:
15
Minuten
Nicht mehr als:
1
Tage
Diese Gültigkeitsdauer-Grenzwerte auch auf Quellen anwenden, die eine Ablaufzeit festlegen
Wiederherstellen
OK
Abbrechen
Übernehmen

Eigenschaften von msisafaq nicht cachen
Allgemein
Nach
Cachespeicher und -abruf
HTTP
FTP
Erweitert
FTP-Zwischenspeicherung aktivieren
Geben Sie den Zeitraum an, in dem FTP-Objekte gültig im Cache sind. Das FTP-Objekt wird ungültig, wenn die Gültigkeitsdauer abläuft.
Gültigkeitsdauer für FTP-Objekte:
1
Tage
Wiederherstellen
OK
Abbrechen
Übernehmen



Nun ist die Regel fertig und die Änderungen können übernommen werden.



Ab sofort werden alle Anfragen an die Webseite www.msisafaq.de nicht zwischengespeichert.

Wann sind solche Maßnahmen sinnvoll?

Erfahrungsgemäß gibt es manchmal Schwierigkeiten, authentifizierte datenbankbasierte Webseiten zwischenzuspeichern. Ebenso können Webseiten mir sehr häufig aktualisiertem Inhalt nicht für die Zwischenspeicherung geeignet sein. Wenn Benutzer Probleme mit einzelnen Webseiten haben, die sich darin äußern, dass die Inhalte nicht dem entsprechen, was mit einer Verbindung ohne ISA Server angezeigt wird, sollte als erster Schritt bei der Fehlersuche versucht werden, die Webseite wie oben beschrieben von der Zwischenspeicherung auszunehmen.

Verteilen der Webproxy-Einstellungen per Gruppenrichtlinie

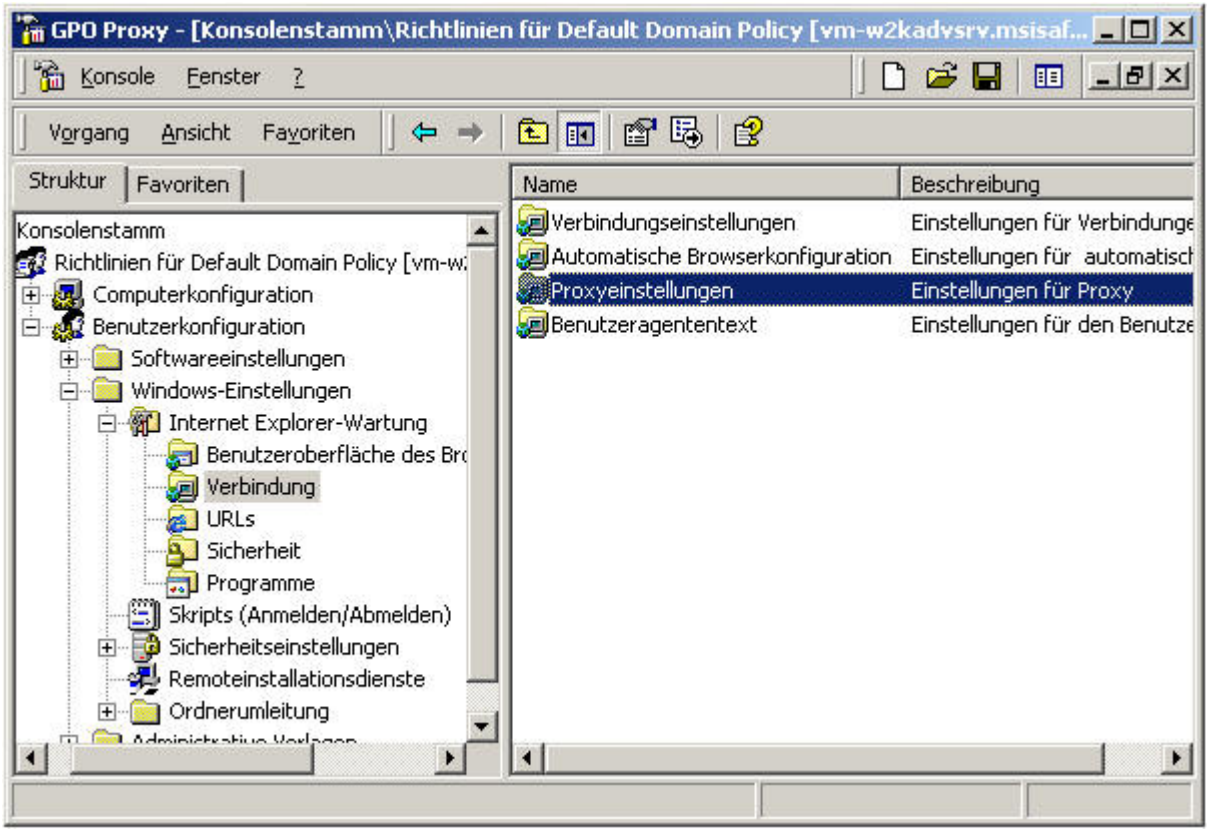
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2000
- Microsoft ISA Server 2004
- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003

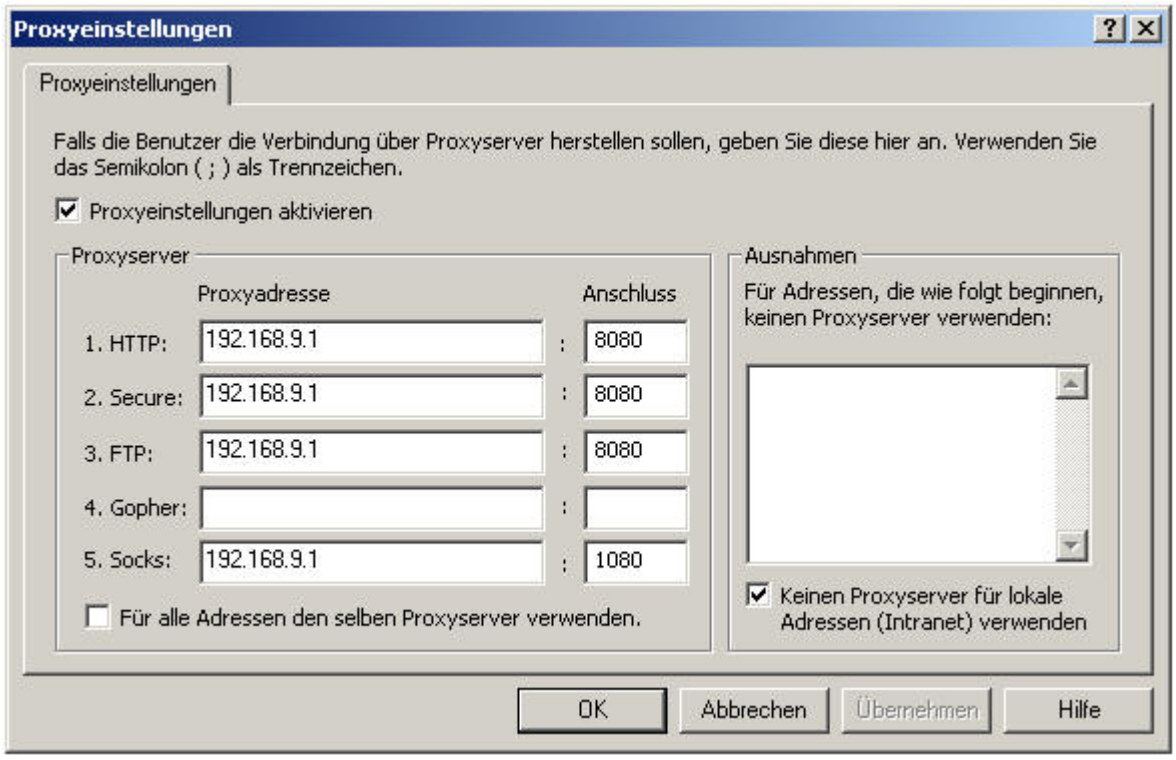
In einem größeren Netzwerk ist es mühsam, an jeder Workstation und für jeden Benutzer von Hand im Internet Explorer die Proxyeinstellungen einzutragen, damit die Workstation zum Webproxyclient wird.

Dies kann - zumindest in einem Windows 2000/2003-Netzwerk mit Active Directory - per Gruppenrichtlinie vordefiniert werden. Alle betroffenen Benutzer bekommen dann automatisch zentral gesteuert die Einstellungen. Besonders ideal ist die Kombination mit WPAD, da hier die größtmögliche Flexibilität erreicht wird.

Je nach Unternehmens- bzw. Netzwerkstruktur kann die Richtlinie auf Domänen- oder Organisationseinheitenebene vergeben werden. Im folgenden Beispiel wird die Default Domain Policy verwendet:

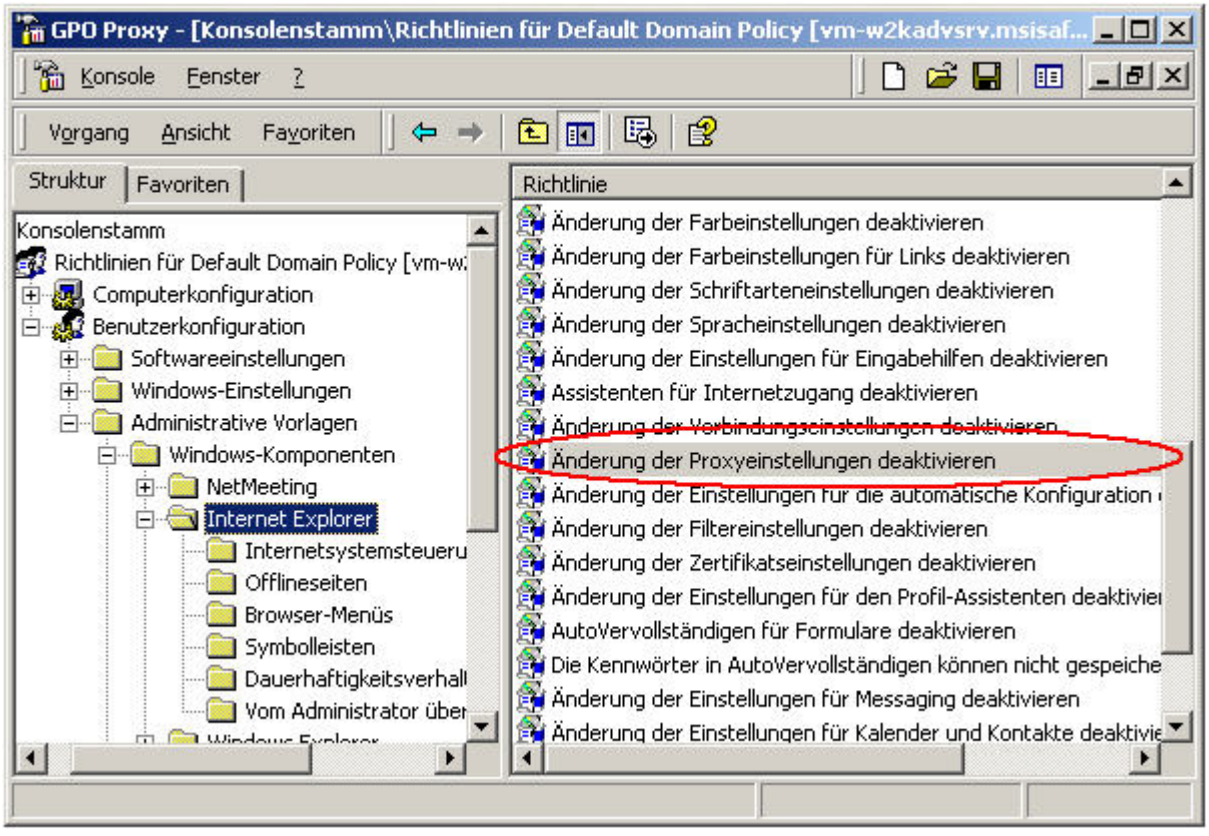


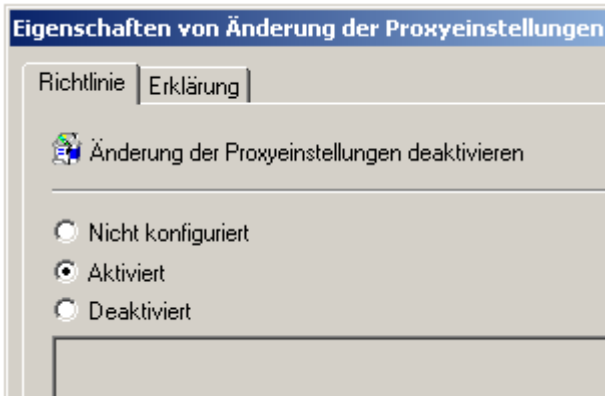
Um einen Proxyserver einzutragen, muss die Richtlinie *Proxyeinstellungen* angepasst werden:



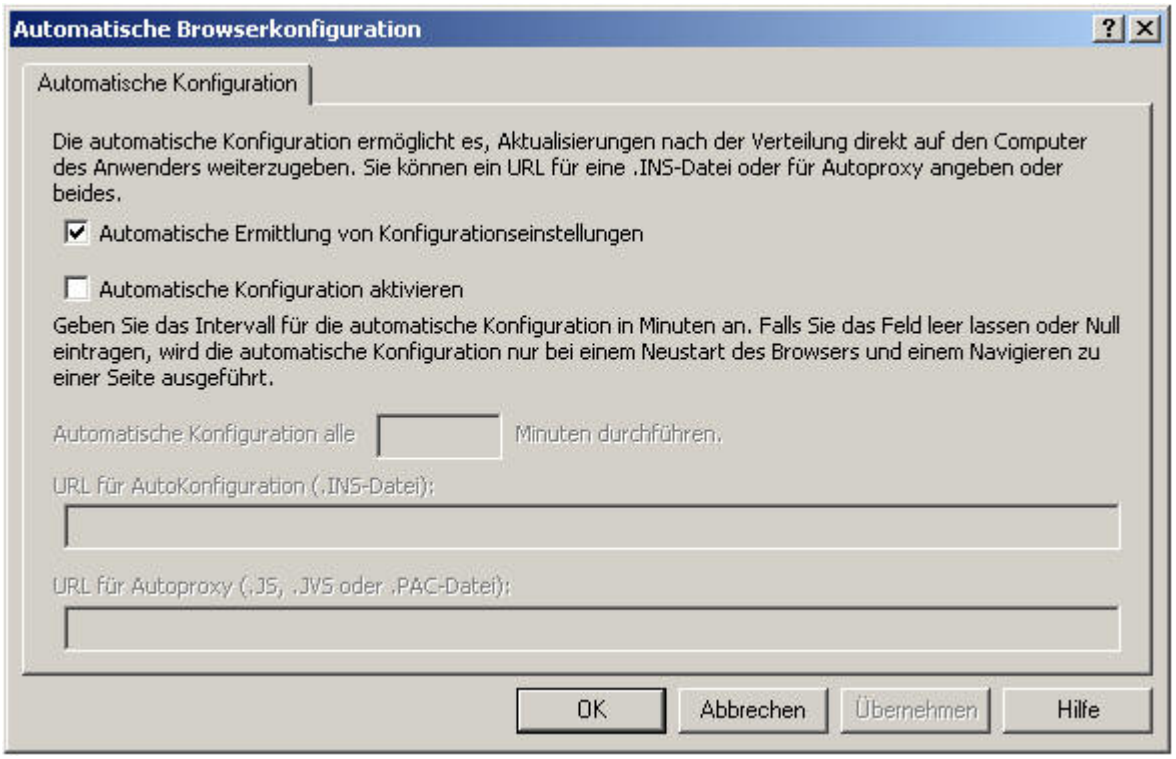
Von nun an erhalten alle angemeldeten Domänenbenutzer die Einstellungen vorkonfiguriert.

Wenn verhindert werden soll, dass die Benutzer die Einstellungen selber verändern, hilft folgende Option:

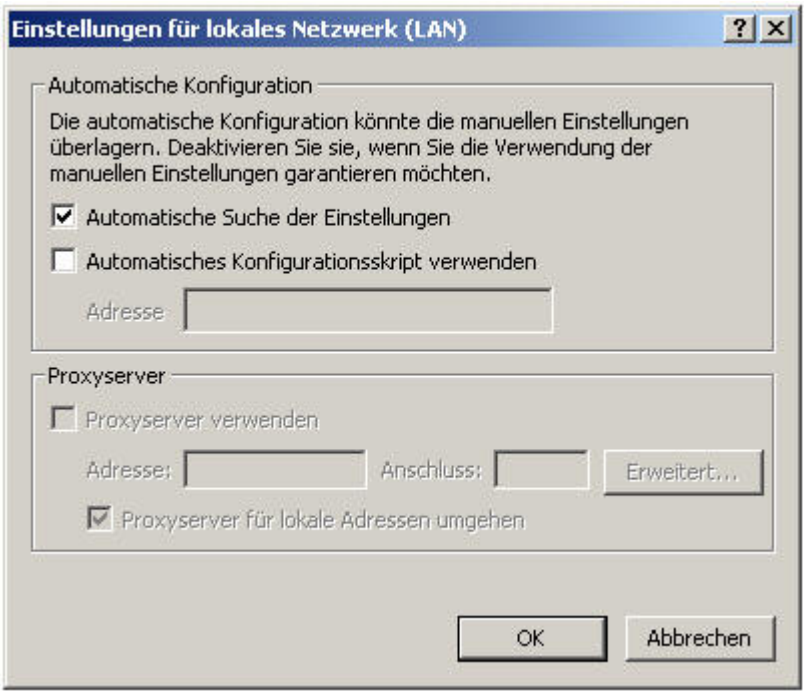




Wenn die Einstellungen zusammen mit WPAD verwendet werden sollen, darf kein Proxy wie oben beschrieben eingetragen werden. In diesem Fall muss die Richtlinie *Automatische Browserkonfiguration* verwendet werden:



Nach der nächsten Anmeldung des Benutzers ist der Internet Explorer wie folgt konfiguriert:


Einstellungen für lokales Netzwerk (LAN)
Automatische Konfiguration
Die automatische Konfiguration könnte die manuellen Einstellungen überlagern. Deaktivieren Sie sie, wenn Sie die Verwendung der manuellen Einstellungen garantieren möchten.
Automatische Suche der Einstellungen
Automatisches Konfigurationsskript verwenden
Adresse
Proxyserver
Proxyserver verwenden
Adresse:
Anschluss:
Erweitert...
Proxyserver für lokale Adressen umgehen
OK
Abbrechen

Socket Pooling bei Windows Server 2003 und ISA Server

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2000
- Microsoft ISA Server 2004
- Microsoft Windows Server 2003

Im Artikel Socket Pooling W2k wurde bereits das Socket Pooling Problem unter Windows 2000 besprochen.

Auch unter Windows Server 2003 und dem IIS 6.0 ist es so, dass standardmäßig die IP-Adresse 0.0.0.0 mit Port 80 an den IIS gebunden ist. Zwar wird der IIS nicht mehr automatisch mitinstalliert und kommt somit dem ISA in der Regel nicht in die Quere, aber in verschiedenen Einsatzzwecken ist es ggfs. erforderlich, dass dennoch auf der ISA Maschine ein IIS installiert ist.

```
C:\Programme\Support Tools>netstat -na | more

Aktive Verbindungen

Proto   Lokale Adresse     Remoteadresse Status
TCP     0.0.0.0:80         0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:135        0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:445        0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:1025       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:1723       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3003       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3004       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3013       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3023       0.0.0.0:0     ABHÖREN
TCP     127.0.0.1:11223    0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:139    0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:1080   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:1745   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:3500   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:3501   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:3502   0.0.0.0:0     ABHÖREN
-- Fortsetzung --
```

Dann wird es erstmal Schwierigkeiten geben, wenn eine Webseite auf Port 80 hören will, denn der ISA beansprucht auch den Port 80. Wenn man jedoch die Webseite auf die internen IP Adresse des ISA konfiguriert und das Socket Pooling abschaltet, stellt dies kein Problem mehr dar.

Um das Socket Pooling abzuschalten sind folgende Schritte notwendig:

1. Socket Pooling für HTTP abschalten:

1. Von der Windows Server 2003 CD aus dem Verzeichnis `<cd:>\support\tools` die "Windows Server 2003-Supporttools " (`suptools.msi`) installieren

```
Z:\SUPPORT\TOOLS>dir
Datenträger in Laufwerk Z: ist W2K3_DE
Volumeseriennummer: 4840-49D1

Verzeichnis von Z:\SUPPORT\TOOLS

26.03.2003 14:00 <DIR> .
26.03.2003 14:00 <DIR> ..
26.03.2003 14:00 1.887.881     DEPLOY.CAB
26.03.2003 14:00 26.624        GBUNICNV.EXE
26.03.2003 14:00 3.649.024     MSRDPCLI.EXE
26.03.2003 14:00 335.360       NETSETUP.EXE
26.03.2003 14:00 3.693.065     SUPPORT.CAB
26.03.2003 14:00 245.760       SUPTOOLS.MSI
26.03.2003 14:00 944.976       SUP_PRO.CAB
26.03.2003 14:00 946.681       SUP_SRV.CAB
8 Datei(en) 11.729.371 Bytes
2 Verzeichnis(se), 0 Bytes frei
```

2. Durch **`net stop http /y`** den IIS HTTP-Dienst anhalten

```
C:\Programme\Support Tools>net stop http /y
Die folgenden Dienste hängen vom Dienst HTTP ab.
Das Beenden des Dienstes HTTP beendet auch diese Dienste.

WWW-Publishingdienst
HTTP-SSL

WWW-Publishingdienst wird beendet.
WWW-Publishingdienst wurde erfolgreich beendet.

HTTP-SSL wird beendet.
HTTP-SSL wurde erfolgreich beendet.

HTTP wurde erfolgreich beendet.
```

3. Durch **`net stop w3proxy`** den ISA Server Webproxydienst anhalten

```
C:\Programme\Support Tools>net stop w3proxy
Microsoft Webproxy wird beendet..
Microsoft Webproxy wurde erfolgreich beendet.
```

4. Aus dem Verzeichnis `c:\programme\support tools\` die Datei `httpcfg.exe` aufrufen:

```
httpcfg delete iplisten -i 0.0.0.0
```

Damit wird der IIS konfiguriert, nicht mehr auf alle IP Adressen zu hören

```
C:\Programme\Support Tools>httpcfg delete iplisten -i 0.0.0.0
HttpDeleteServiceConfiguration completed with 1168.
```

5. Anschließend die IP festlegen, auf die der IIS hören soll:

`httpcfg set iplisten -i 172.16.19.1`

Wobei 172.16.19.1 nur als Beispiel dienen soll

```
C:\Programme\Support Tools>httpcfg set iplisten -i
172.16.19.1
HttpSetServiceConfiguration completed with 0.
```

6. Mit **`net start http`** den IIS HTTP-Dienst starten

```
C:\Programme\Support Tools>net start http
HTTP wurde erfolgreich gestartet.
```

7. Mit **`net start w3svc`** den IIS WWW Dienst neu starten

```
C:\Programme\Support Tools>net start w3svc
WWW-Publishingdienst wird gestartet.
WWW-Publishingdienst wurde erfolgreich gestartet.
```

8. Mit **`net start w3proxy`** den ISA Server Webproxydienst neu starten

```
C:\Programme\Support Tools>net start w3proxy
Microsoft Webproxy wird gestartet.
Microsoft Webproxy wurde erfolgreich gestartet.
```

Anschließend gehört die 0.0.0.0 nicht mehr dem IIS:

```
C:\Programme\Support Tools>netstat -na | more

Aktive Verbindungen

Proto   Lokale Adresse     Remoteadresse Status
TCP     0.0.0.0:135        0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:445        0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:1025       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:1723       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3003       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3004       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3013       0.0.0.0:0     ABHÖREN
TCP     0.0.0.0:3023       0.0.0.0:0     ABHÖREN
TCP     127.0.0.1:11223    0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:139    0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:1080   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:1745   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:3500   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:3501   0.0.0.0:0     ABHÖREN
TCP     172.16.19.1:3502   0.0.0.0:0     ABHÖREN
-- Fortsetzung --
```

2. Deaktivieren des Socket Pooling für FTP

Es sind folgende Schritte notwendig (in einem Kommandozeilenfenster):

1. `cd c:\Inetpub\AdminScripts`
2. `net stop msftpsvc`
3. `cscript adsutil.vbs set msftpsvc/disablesocketpooling true`
4. `net start msftpsvc`

3. Deaktivieren des Socket Pooling für SMTP

Es sind folgende Schritte notwendig (in einem Kommandozeilenfenster):

1. `cd c:\Inetpub\AdminScripts`
2. `net stop smtpsvc`
3. `cscript adsutil.vbs set smtpsvc/disablesocketpooling true`
4. `net start smtpsvc`

4. Deaktivieren des Socket Pooling für POP3

Es sind folgende Schritte notwendig (in einem Kommandozeilenfenster):

1. `cd c:\Inetpub\AdminScripts`
2. `net stop pop3svc`
3. `cscript adsutil.vbs set pop3svc/disablesocketpooling true`
4. `net start pop3svc`

5. Deaktivieren des Socket Pooling für IMAP

Es sind folgende Schritte notwendig (in einem Kommandozeilenfenster):

1. `cd c:\Inetpub\AdminScripts`
2. `net stop imap4svc`
3. `cscript adsutil.vbs set imap4svc/disablesocketpooling true`
4. `net start imap4svc`

DNS Auflösung

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004
- Windows 2000 Server
- Windows Server 2003

Eine korrekt funktionierende DNS-Auflösung ist ein wesentlicher Bestandteil einer jeden ISA Server Installation. Unabhängig davon, dass ein Active Directory unter Windows 2000 bzw. Windows Server 2003 nicht ohne DNS auskommt ist es für die Ansteuerung von Servern im Internet unverzichtbar.

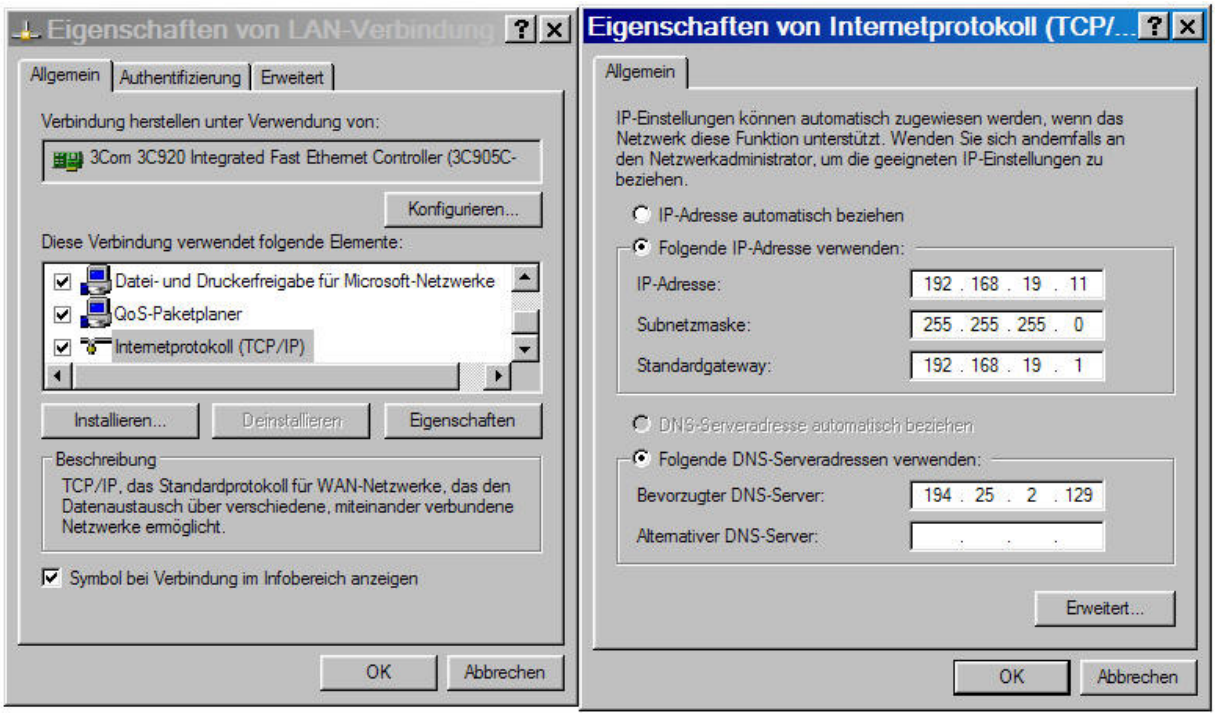
Im folgenden Artikel möchte ich keine DNS-Implementierung im AD besprechen, sondern mich rein auf den Zusammenhang mit dem ISA Server beschränken. Literatur zu DNS und AD gibt es genügend [1]. Viele Probleme, die mich immer wieder erreichen oder in der Newsgroup geschildert werden haben unmittelbar mit einem DNS Problem zu tun. Sei es der Mailserver, der keine Mails zustellen kann, keine Client-Pop3-Abfragen oder Probleme, Webseiten aufzurufen. Dabei ist DNS im Grunde sehr einfach. Man muss sich nur überlegen, wie man DNS implementieren will. Wie immer im Leben gibt es auch hier verschiedene Wege zum Ziel. Hinzu kommt noch, dass der ISA Server je nach Clienttyp anders reagiert. Für einen Firewallclient kümmert sich der ISA selber um sämtliche Namensauflösungen, d.h. der ISA selber muss in der Lage sein, korrekte DNS-Abfragen beantwortet zu bekommen. Bei einem SecureNAT Client ist der jeweilige Client eigenverantwortlich. Hier muss sichergestellt werden, dass dieser - unabhängig vom ISA Server - in der Lage ist, Namen aufzulösen.

Welche Möglichkeiten gibt es nun, DNS zu verwenden?

1. Jeder Client bekommt einen externen DNS Server (statisch oder per DHCP) zugewiesen
2. Jeder Client bekommt nur den internen AD-DNS zugewiesen
3. Jeder Client bekommt den internen AD-DNS und einen weiteren externen DNS-Server zugewiesen

Jeder Client bekommt einen externen DNS Server (statisch oder per DHCP) zugewiesen

Ein mögliches Szenario wäre, jedem internen Client in den LAN-Einstellungen einen externen DNS-Server einzutragen.



Natürlich kann der DNS-Server auch per DHCP-Optionen verteilt werden:

Diese Methode hat den Nachteil, dass jeder Client ständig übers Internet DNS-Anfragen starten muss. Dies vermindert die Bandbreite und produziert unnötigen Datenverkehr. In kleinen Netzen mit wenigen PC´s und ohne eigenem DNS-Server könnte es unter Umständen Sinn machen. Aber nur dort...

Damit auch jeder Client eigene DNS Anfragen durch den ISA los wird, muss im ISA eine Firewallrichtlinie für DNS vorhanden sein:

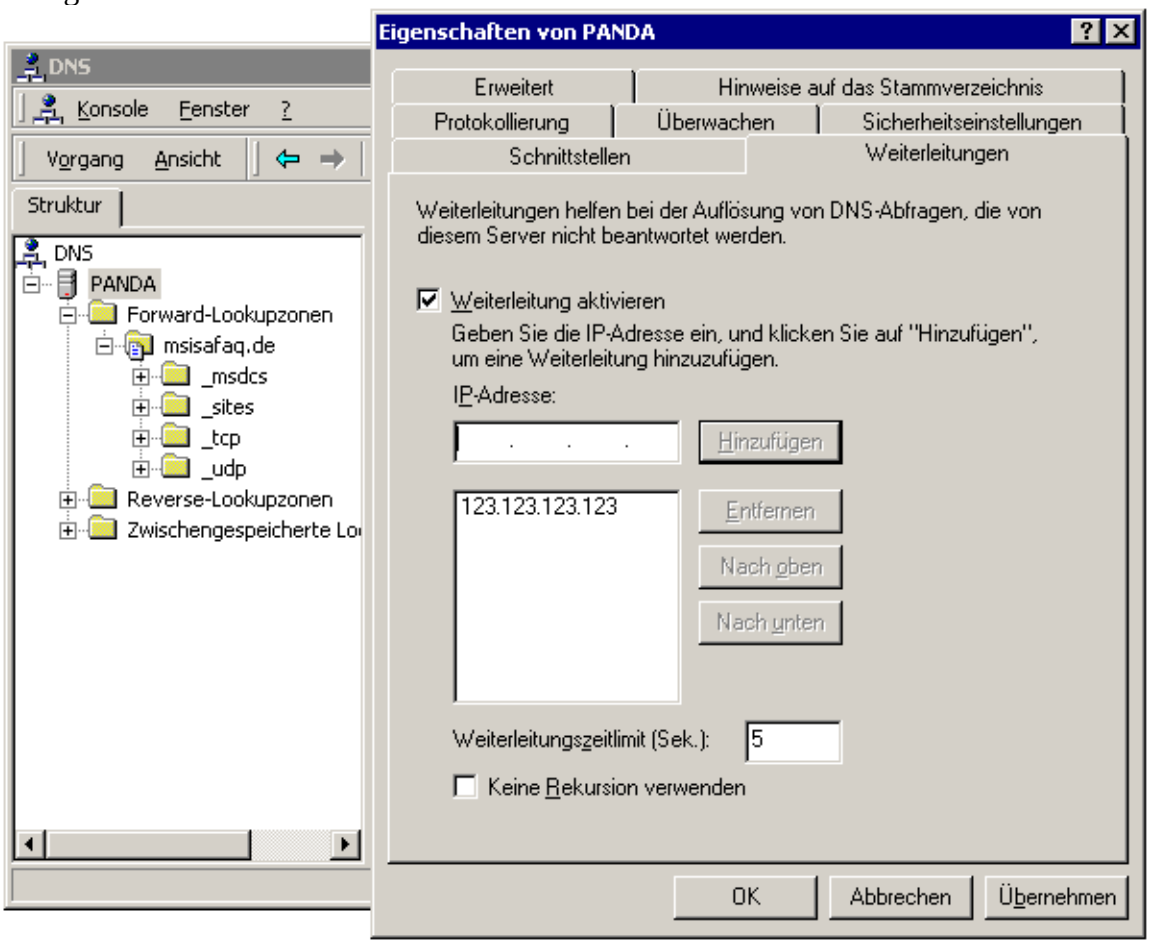
Jeder Client bekommt nur den internen AD-DNS zugewiesen

Wenn ein Active Directory vorhanden ist, benötigen die Clients sowieso den internen AD-DNS Server als primären DNS-Server. Am besten verteilt man das wieder per DHCP.

Warum DHCP?
Ich verwende in den meisten Netzwerken sehr gerne DHCP für sämtliche Clients, Drucker und ggfs. Mitgliedserver. Dadurch werden Netzwerkänderungen zum Kinderspiel. Nicht mehr jeder einzelne Rechner muss angefasst werden, wenn sich etwas ändert (z.B. ein neues Default Gateway oder ein DNS Server). Ein weiterer Vorteil ist die zentrale Kontrolle und Administration über einen Server. Man kann ohne Probleme einzelne Optionen dadurch verteilen (siehe oben). Und selbst wenn der DHCP-Server zum Zeitpunkt der Anmeldung des Clients nicht vorhanden ist - der kann eine einstellbare Zeit die zugewiesene IP Adresse behalten.

Also muss der Client, wenn er z.B. www.msisafaq.de auflösen möchte, den AD-DNS fragen. Woher bekommt/holt sich dieser DNS Server die Information? Hier gibt es wiederum zwei denkbare Ansätze, dies zu realisieren.

- Der AD-DNS Server hat eine Weiterleitung zu einem externen DNS Server (z.B. des Internet Service Providers) eingetragen und befragt somit diesen. Dies wird hier konfiguriert:



Sollte der Punkt "Weiterleitung aktivieren" ausgegraut sein, dann ist die Root (Forward-Lookup)Zone (".") vorhanden. Die muss dann entfernt werden. Nach einem Neustart des DNS Servers kann die Weiterleitung aktiviert werden.

Da die Clients nun nicht mehr direkt externe DNS Server anfragen, kann man im ISA Server den Zugriff auf das Protokoll "DNS" durch einen Computerobjekt einschränken.

- Wenn es das allgemeine Netzwerkdesign zulässt, verwende ich einen weiteren Schritt in der Namensauflösung. Wenn zum Beispiel mehrere Domaincontroller vorhanden sind, leite ich die DNS-Server an einen weiteren internen Server weiter. Dies kann zum Beispiel der ISA Server selber sein. Nur dieser eine darf dann DNS-Anfragen stellen. Der DNS-Server erhält statt der Weiterleitung zu einer externen IP-Adresse (wie oben) eine interne IP eingetragen.

  Am ISA muss dazu eine Regel erstellt werden, die dem DC eine Verbindung zum lokalen DNS Server erlaubt.

Mittels der vorhandenen Systemrichtlinie darf der ISA Server selber DNS Anfragen an das externe Interface stellen:

Jeder Client bekommt den internen AD-DNS und einen weiteren externen DNS-Server zugewiesen

Bei den Vorbereitungen zu diesem Artikel ist mir auch diese Lösung eingefallen. Möchte sie nur der Vollständigkeit halber erwähnen - empfehle sie nicht. Der Verwaltungsaufwand ist zu hoch. Von der Konfiguration ist es eine Mischung aus den beiden vorgenannten Möglichkeiten. Hierbei muss sichergestellt werden, dass ein eventuell vorhandener Exchange-Server DNS-Abfragen stellen kann.

Geplante Inhaltsdownloadsaufträge einrichten

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

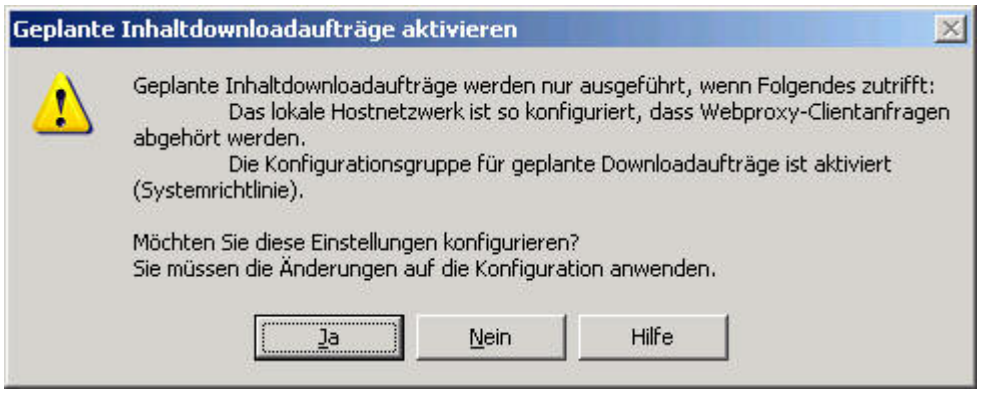
Neben der Cachefunktion für häufig abgerufene Webinhalte kann der ISA Server 2004 zur Performancesteigerung automatisiert bestimmte Webseiten zeitgesteuert in den Cache laden.

Das kann in bestimmten Fällen Vorteile haben:

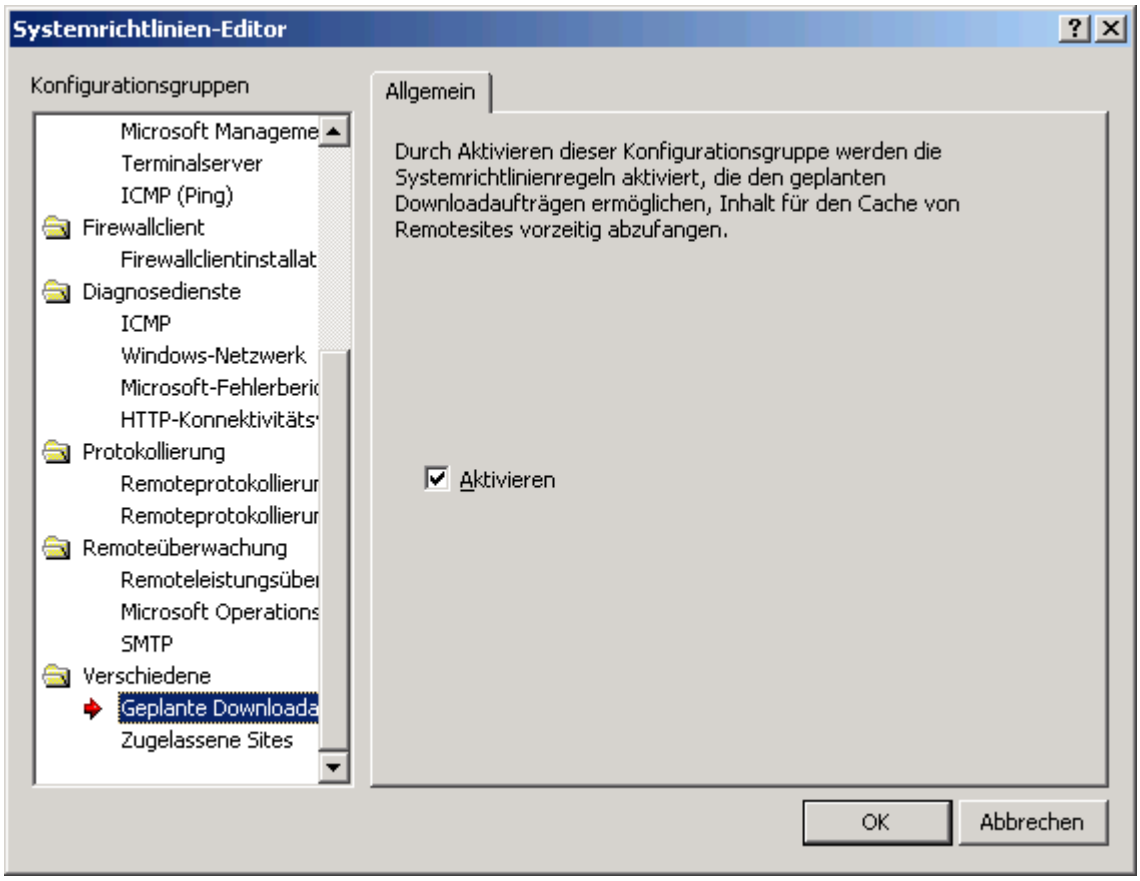
- schnellere Bereitstellung des Inhalts für die Clients, da keine "echte" Anforderung an den Zielserver gesendet wird
- es kann eine Zeitspanne verwendet werden, in der mehr Bandbreite zur Verfügung steht (Nacht)

Im Kontextmenü oder im Aufgabenbereich des Knotens "Cache" steht der Menüpunkt "Neuer Inhaltsdownloadauftrag" zur Verfügung.

Beim ersten Aufruf erscheint folgender Hinweis:

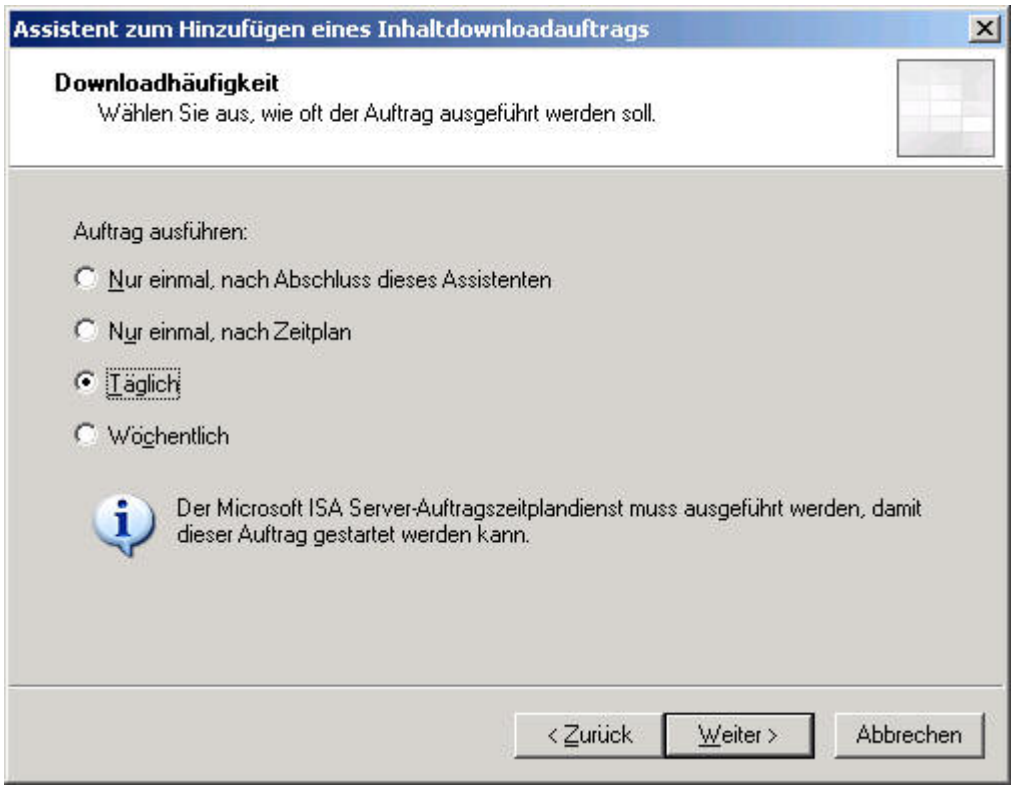


Dadurch wird in der Systemrichtlinie der Downloadauftrag zugelassen:

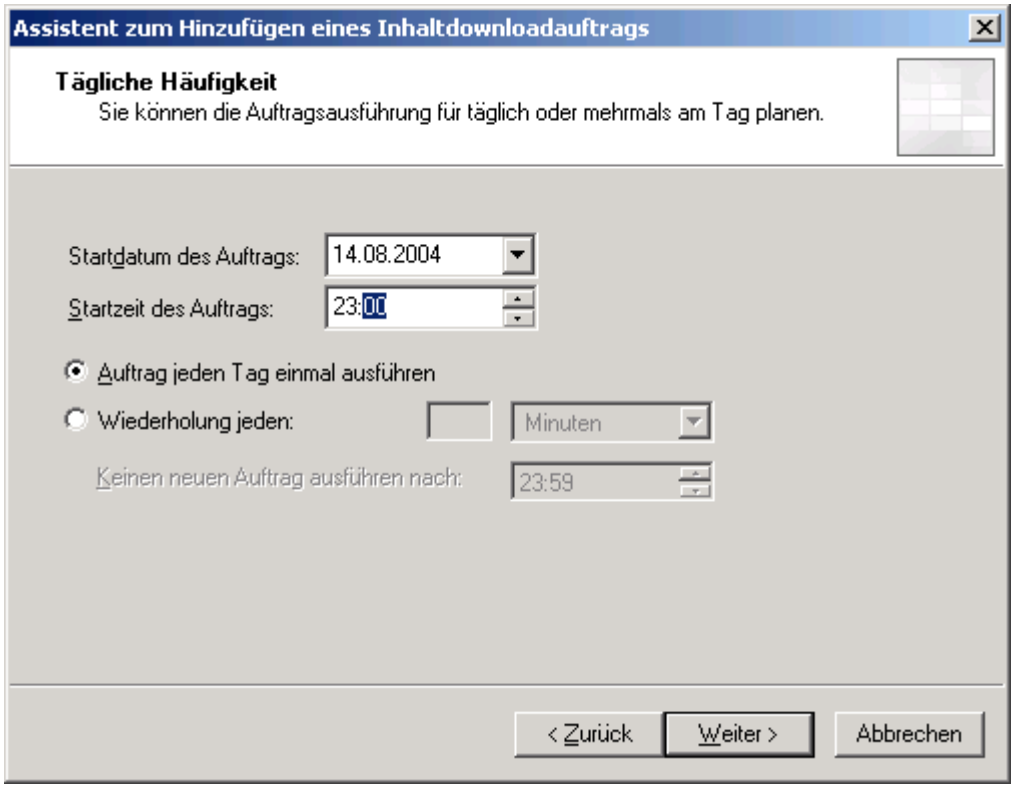


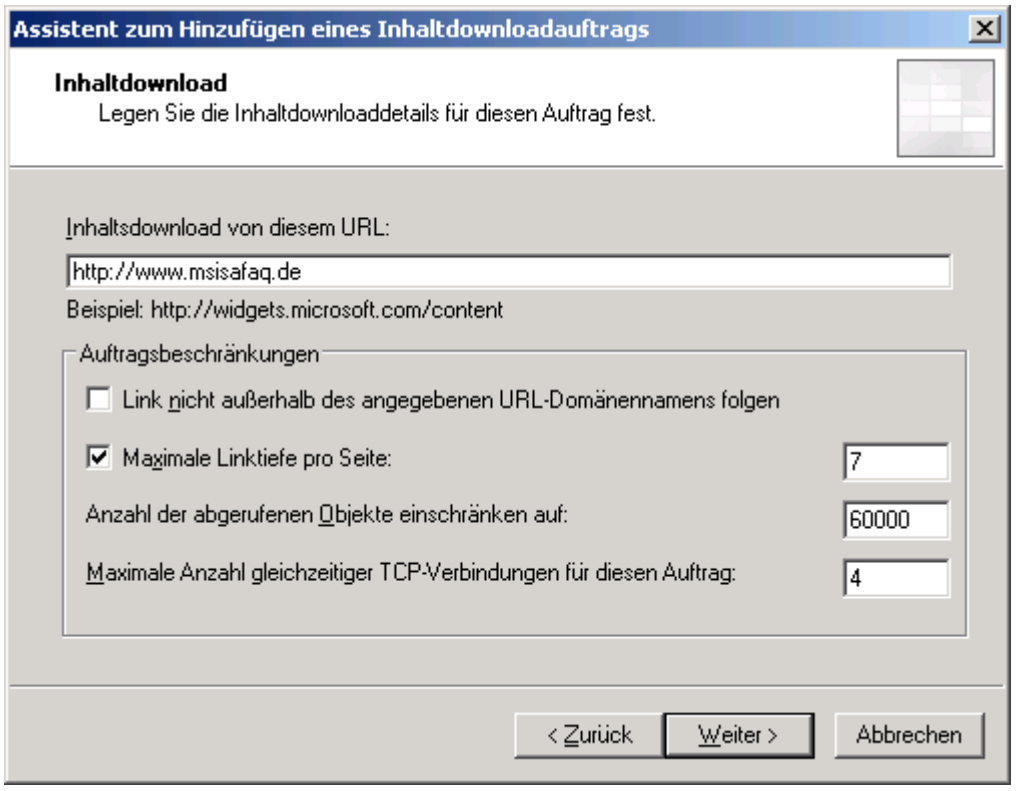
Zusätzlich muss in einer weiteren, übergeordneten Zugriffsregel nicht authentifizierter HTTP-Zugriff vom lokalen Hostnetzwerk zugelassen werden. Je nach Konfigurationsstand des ISA Servers muss vor der weiteren Regelerstellung zuerst die Änderung übernommen werden.

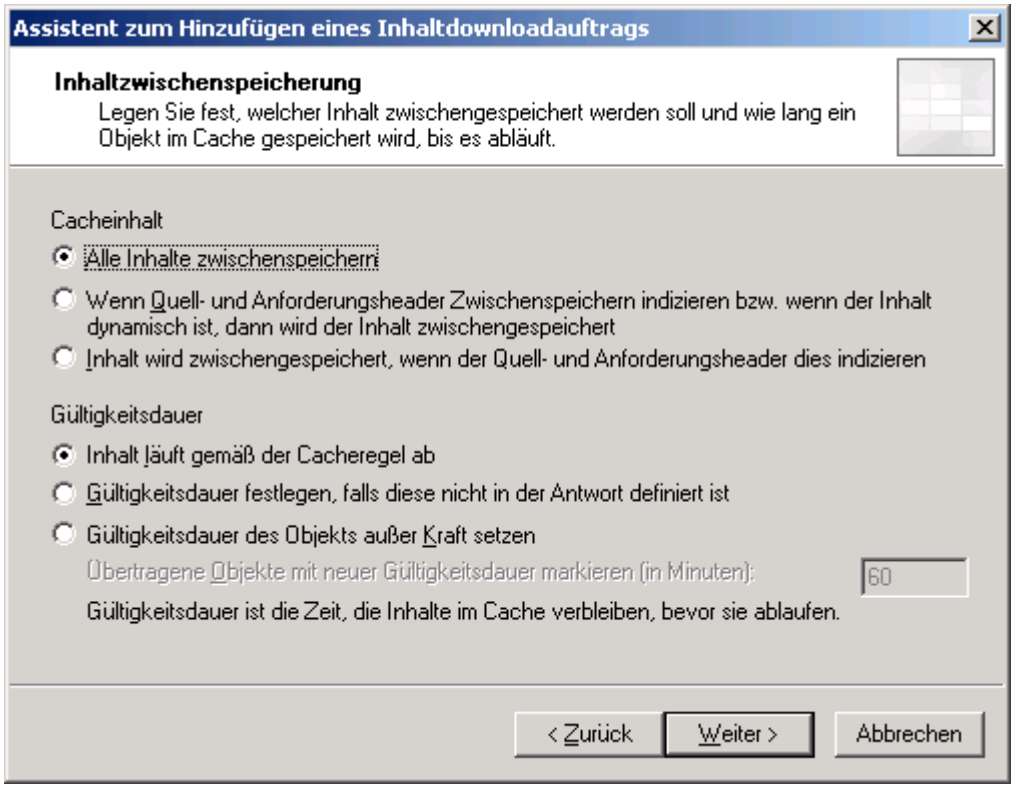
Anschließend muss man den Regelassistent erneut starten.



Hier kann angegeben werden, wie oft der Auftrag ausgeführt werden soll. Im nächsten Dialog kann das noch - in Abhängigkeit der letzten Angabe - verfeinert werden:


Assistent zum Hinzufügen eines Inhaltdownloadauftrags
Tägliche Häufigkeit
Sie können die Auftragsausführung für täglich oder mehrmals am Tag planen.
Startdatum des Auftrags:
14.08.2004
Startzeit des Auftrags:
23:00
Auftrag jeden Tag einmal ausführen
Wiederholung jeden:
Minuten
Keinen neuen Auftrag ausführen nach:
23:59
< Zurück
Weiter >
Abbrechen


Assistent zum Hinzufügen eines Inhaltdownloadauftrags
Inhaltdownload
Legen Sie die Inhaltdownloaddetails für diesen Auftrag fest.
Inhaltsdownload von diesem URL:
http://www.msisafaq.de
Beispiel: http://widgets.microsoft.com/content
Auftragsbeschränkungen
Link nicht außerhalb des angegebenen URL-Domänennamens folgen
Maximale Linktiefe pro Seite:
7
Anzahl der abgerufenen Objekte einschränken auf:
60000
Maximale Anzahl gleichzeitiger TCP-Verbindungen für diesen Auftrag:
4
< Zurück
Weiter >
Abbrechen



Um die Gültigkeitsdauer (TTL) für ein Objekt außer Kraft zu setzen, aktivieren Sie das Kontrollkästchen "Gültigkeitsdauer des Objekts außer Kraft setzen". Um die Gültigkeitsdauer für ein Objekt vorzugeben, wenn keine Gültigkeitsdauer definiert ist, aktivieren Sie das Kontrollkästchen "Gültigkeitsdauer festlegen, falls diese nicht in der Antwort definiert ist". Um eine bestimmte Gültigkeitsdauer für gedownloadete Objekte zu konfigurieren, geben Sie unter Übertragene Objekte mit neuer Gültigkeitsdauer markieren (in Minuten): Anzahl eine Gültigkeitsdauer ein.

Anmerkungen:

- Wenn der Cacheinhaltdownloadauftrag fehlschlägt, wird ein Ereignis in der Windows-Ereignisanzeige protokolliert.
- Der geplante Inhaltdownloadauftrag schlägt fehl, wenn vom Webserver, von dem das Objekt gedownloadet wird, eine Clientauthentifizierung gefordert wird.

Benutzerauthentifizierung bei ausgehenden Webanfragen

Die Informationen in diesem Artikel beziehen sich auf:

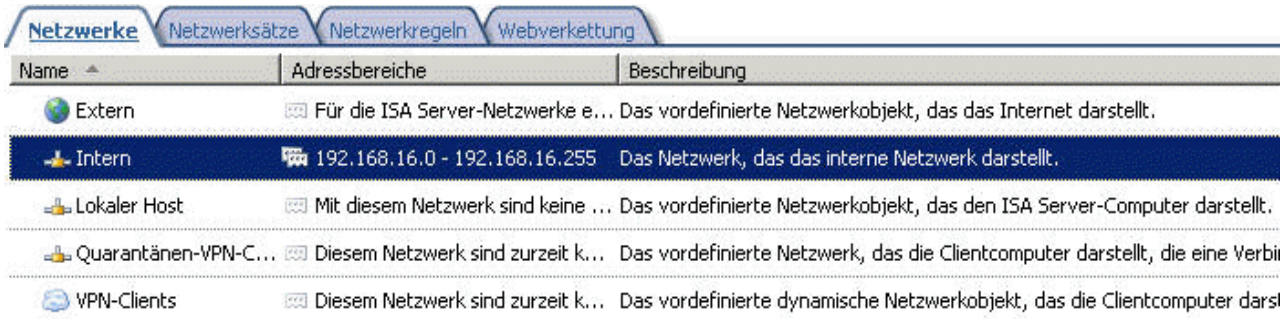
- Microsoft ISA Server 2004

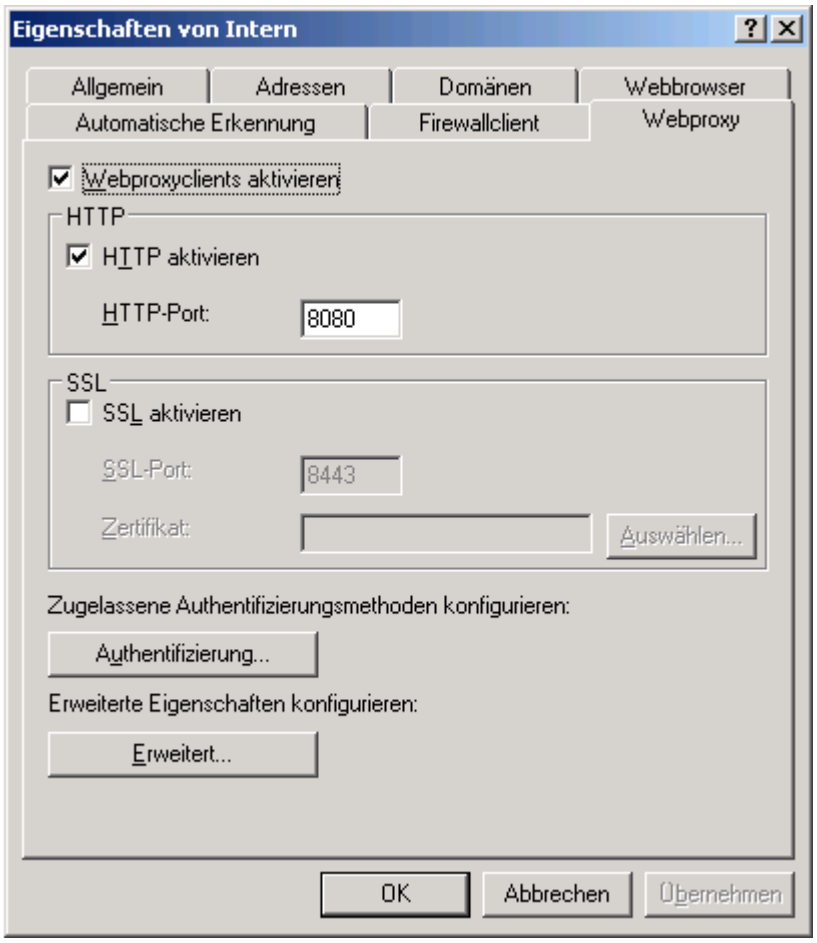
Oftmals ist es erforderlich, dass für ausgehende Webanfragen (also Anfragen über http, https und ftp) eine Zugriffskontrolle auf Benutzerebene erfolgen kann. In vielen Unternehmen wird aus arbeitsrechtlichen- oder aus Sicherheitsgründen nicht allen Mitarbeitern ein uneingeschränkter Internetzugang ermöglicht. Um das zu Kontrollieren ist der ISA Server bestens geeignet. Der ISA Server kann grundsätzlich bei allen Zugriffsarten Regeln pro IP-Adresse oder pro Benutzer freigeben. Standardmäßig ist keine Benutzerauthentifizierung aktiviert.

Benutzerauthentifizierung kann an mehreren Stellen verwendet werden. Sobald der Firewallclient installiert ist, können für alle nicht-Webprotokolle benutzerabhängige Zulassungsregeln erstellt werden. Somit kann z.B. erreicht werden, dass für Benutzer Birgit von jedem Rechner aus ausgehende SMTP Anfragen erlaubt sind. Ohne den Firewallclient würde dies nur über Clientadresssätze und somit nur basierend auf einer oder mehreren IP-Adresse möglich sein.

Damit auch für die Webprotokolle http, https und ftp eine Benutzerauthentifizierung möglich wird, muss der Webproxyclient verwendet werden. Sowohl der Firewallclient als auch der SecureNAT-Client scheitern am Webproxyfilter. Zuvor muss natürlich der ISA Server für die Benutzerauthentifizierung konfiguriert werden.

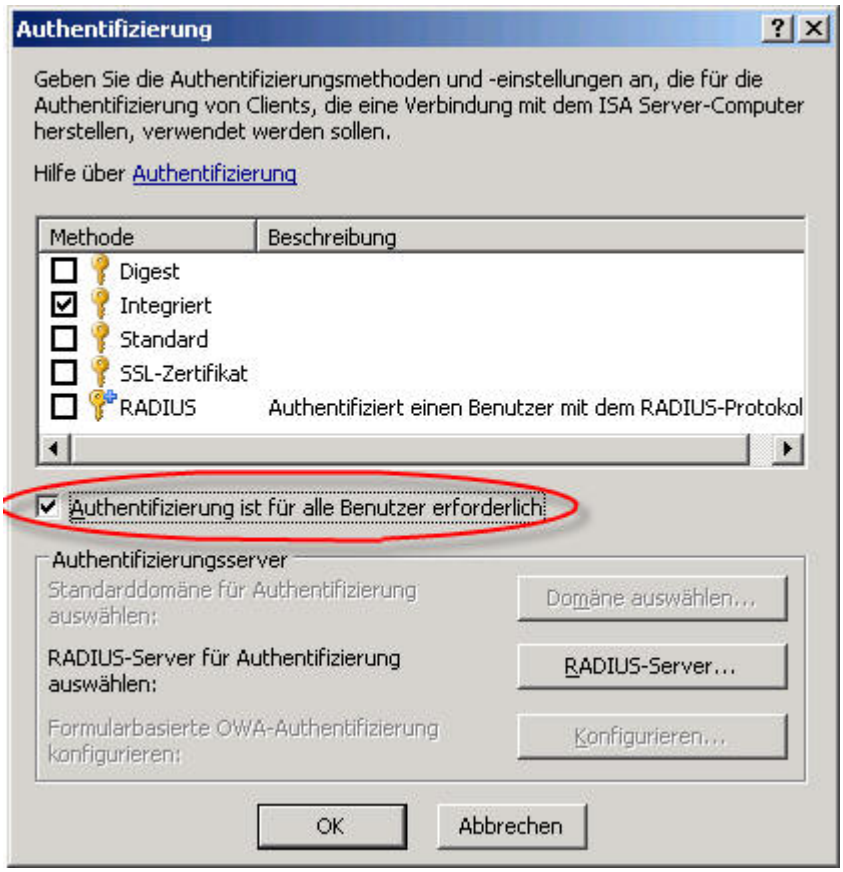
Dazu muss man im Knoten *Netzwerke* in die Eigenschaften des internen Netzwerkes gehen:





In der Registerkarte "Webproxy" kann man den Webproxy für dieses Netzwerk aktivieren und den Abhörport (Listener) konfigurieren. Standard ist Port 8080.

Über die Schaltfläche "Authentifizierung..." gelangt man zu folgenden Optionen:



Über den Schalter *Authentifizierung ist für alle Benutzer erforderlich* wird die Authentifizierung für das ganze interne Netzwerk eingeschaltet.

Hinweis: Wird der Schalter "Authentifizierung ist für alle Benutzer erforderlich" nicht aktiviert, kann dennoch eine Benutzerauthentifizierung erzwungen werden. Wenn eine Regel für http/ftp mit einer Gruppe existiert, gilt diese auch nur für die Gruppenmitglieder. Unabhängig vom gesetzten Schalter. Es ist daher immer wichtig, die richtige Authentifizierungsmethode zu verwenden. In einer reinen Windows-Umgebung sollte die Integrierte Authentifizierung aktiviert sein.

Im oben abgebildeten Fall haben die Mitglieder der Gruppe Administratoren uneingeschränkten Internetzugriff. Alle anderen Benutzer dürfen nur die Webseiten aufrufen, die durch die Systemrichtlinie erlaubt sind.

Je nach vorhandener Netzwerkumgebung muss jedoch die Authentifizierungsmethode angepasst werden. Dies ist zum Beispiel der Fall wenn als Webbrowser nicht der Microsoft Internet Explorer (ab 5.x) verwendet wird. Die anderen Browser unterstützen nämlich die Integrierte Authentifizierung nicht.

Hier eine kurze Zusammenstellung der fünf angebotenen Authentifizierungsmethoden (Auszug aus der Online-Hilfe):

- **Standardauthentifizierung**
  HTTP verwendet als Standardauthentifizierungsmethode die Standardauthentifizierung. Die Standardauthentifizierung sendet und empfängt Benutzerinformationen als leicht lesbare Textzeichen. Während Kennwörter und Benutzernamen verschlüsselt werden, wird bei der Standardauthentifizierung keine Verschlüsselung verwendet. Im Folgenden wird das Authentifizierungsverfahren bei der Standardauthentifizierung beschrieben:
  1. Der Client fordert den Benutzer auf, Benutzername und Kennwortinformationen einzugeben.
  2. Die Anmeldeinformationen werden anschließend vom Client verschlüsselt und an den Server gesendet.
  3. Für den Benutzernamen wird das Vorhandensein eines Kontos auf dem Microsoft Internet Security & Acceleration Server-Computer (ISA Server) oder in einer vertrauten Domäne des ISA Servers überprüft.

- **Digestauthentifizierung**
  Die Digestauthentifizierung bietet dieselben Funktionen wie die Standardauthentifizierung, die Authentifizierungsinformationen werden jedoch auf andere Weise übertragen. Die Authentifizierungsinformationen durchlaufen einen Einwegprozess, der oft als Hashprozess bezeichnet wird. Das Ergebnis dieses Prozesses wird Hashwert oder Nachrichten-Hash genannt. Es kann nicht entschlüsselt werden, d. h. der ursprüngliche Text kann nicht aus dem Hashwert entziffert werden.

  Vor dem Hashprozess werden zusätzliche Informationen zum Kennwort hinzugefügt, sodass niemand den Kennworthashwert erfassen und zur Nachahmung des echten Benutzers verwenden kann. Es werden Werte hinzugefügt, die bei der Identifizierung des Benutzers, des Computers und der dazugehörigen Domäne helfen. Um zu verhindern, dass ein widerrufenes Kennwort verwendet wird, wird hier eine Zeitmarkierung hinzugefügt. Dies ist ein deutlicher Vorteil gegenüber der Standardauthentifizierung, da das Kennwort nicht abgefangen und von einer unberechtigten Person verwendet werden kann.

  Die Digestauthentifizierung kann nur in Windows 2000-Domänen verwendet werden.

- **Integrierte Windows-Authentifizierung**
  Die integrierte Windows-Authentifizierung ist eine sichere Form zur Benutzerauthentifizierung, da der Benutzername und das Kennwort nicht über das Netzwerk gesendet werden. Die integrierte Windows-Authentifizierung kann entweder das Kerberos V5-Authentifizierungprotokoll oder das eigene Herausforderung/Rückmeldung-Authentifizierungsprotokoll verwenden.

- **SSL-Zertifikat**
  Sie können die Secure Sockets Layer (SSL)-Sicherheitsfunktionen zur Authentifizierung verwenden. Wenn ein Client ein Objekt von einem Server anfordert, gibt es zwei Möglichkeiten zur Zertifizierung:
  - Der Server authentifiziert sich selbst, indem er ein Serverzertifikat an den Client sendet.
  - Der Server fordert den Client auf, sich zu authentifizieren. In diesem Fall muss der Client dem Server ein geeignetes Clientzertifikat präsentieren.

SSL führt die Authentifizierung durch, indem während des Anmeldeprozesses der Inhalt einer verschlüsselten digitalen Identifikation vom Webbrowser des Benutzers überprüft wird. (Die Benutzer erhalten ihre Clientzertifikate von einer externen Organisation, der beide vertrauen.) Die Serverzertifikate enthalten identifizierende Informationen über den Server. In den Clientzertifikaten sind normalerweise identifizierende Informationen über den Benutzer und die Organisation, von der das Zertifikat ausgestellt wurde, enthalten.

- **RADIUS**
  RADIUS (Remote Authentication Dial-In User Service) ist ein Industriestandardprotokoll, das in RFC 2865, "Remote Authentication Dial-in User Service (RADIUS)", beschrieben ist. Das RADIUS-Protokoll dient zur Authentifizierung. Ein RADIUS-Client (in der Regel ein DFÜ-Server, VPN-Server oder Drahtloszugriffspunkt) sendet Benutzeranmeldeinformationen und Verbindungsparameterinformation in Form einer RADIUS-Nachricht an einen RADIUS-Server. Der RADIUS-Server authentifiziert die RADIUS-Clientanforderung und sendet eine RADIUS-Nachrichtenantwort zurück.

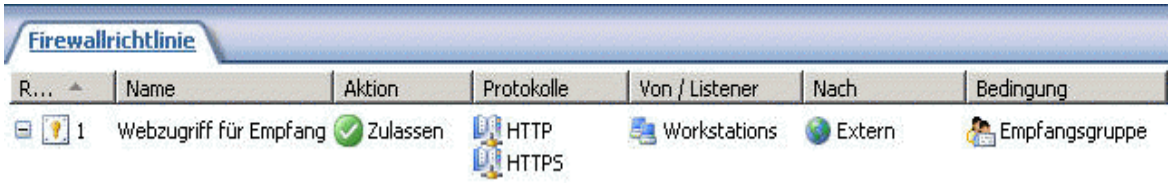
  Clientanmeldeinformationen werden durch RADIUS-Server nicht nur authentifiziert, sondern auch autorisiert. Wenn daher ISA Server vom RADIUS-Server eine Antwort erhält, gemäß der die Clientanmeldeinformationen nicht zugelassen werden, kann dies auch bedeuten, dass der RADIUS-Server den Client nicht autorisieren konnte. Selbst nach erfolgter Authentifizierung der Anmeldeinformationen kann ISA Server eine Clientanforderung unter Umständen auf Grundlage der Autorisierungsrichtlinie des RADIUS-Servers ablehnen.

Anmerkung: RADIUS-Benutzer müssen Anmeldeinformationen im Format Domäne\Benutzer (und nicht als Benutzer@Domäne) an ISA Server übergeben.

Sie können ISA Server so konfigurieren, dass für die RADIUS-Benutzerauthentifizierung bestimmte RADIUS-Server verwendet werden.

RADIUS-Authentifizierung für ausgehende Anforderungen
Bei Verwendung von IAS (Internet Authentication Service) als RADIUS-Server müssen Sie im Einwählprofil der RAS-Richtlinie von IAS die unverschlüsselte Authentifizierung aktivieren, d. h. PAP (Password Authentication-Protokoll) oder SPAP (Shiva Password Authentication-Protokoll). Die Aktivierung von IAS für PAP oder SPAP ist eine profilbasierte IAS-Einstellung. Alle RADIUS-Clients, die diese Richtlinienbedingungen erfüllen, können dann eine Verbindung zum IAS-Server über PAP oder SPAP herstellen.

Nun kann eine Richtlinie, die eines der Webprotokolle zulässt auf Benutzer oder Gruppen eingeschränkt werden.



RADIUS/IAS Authentifizierung mit dem ISA Server 2004

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

Der ISA 2004 bietet als erste Firewalllösung von Microsoft die Möglichkeit, eine Benutzerauthentifizierung für das Regelwerk über eine RADIUS (Remote Authentication Dial-In User Service) Verbindung einzurichten.

Die Microsoft Implementierung von RADIUS nennt sich IAS (Internet Authentication Service) und steht unter Windows 2000 und 2003 für alle Windows Versionen (Ausnahme Windows 2003 Web Editon), zur Verfügung.

Nachteile der IAS Authentifizierung mit dem ISA Server 2004

- RADIUS Traffic ist per Default unverschlüsselt. Die Verwendung von IPSEC wird empfohlen
- Bei jedem zutreffen der Regel muss RADIUS den Client reauthentifizieren, was bei ausgelasteten Servern mehr Netzwerk- und Verarbeitungslast erzeugt.
- ISA enthält nicht sehr viele Informationen im RADIUS Access-Request Paket, so dass eine Unterscheidung zwischen ISA und anderen Diensten sehr schwer ist, wenn alle auf derselben Maschine laufen.

Hinweis: *Webbrowser verstehen kein RADIUS als Authentifizierungstyp, so dass der ISA Server 2004 den Clint auffordert sich per Basic Authentication zu identifizieren. ISA packt diese Pakete in ein RADIUS Access Request Paket und sendet diese zum ausgewählten RADIUS Server.*

Warum RADIUS/IAS

Ein ISA 2004 Server befindet sich oftmals in einer DMZ (DeMilitarisierten Zone). Dabei handelt es sich um einen Hochsicherheitsbereich welcher nur die notwendigsten Verbindungen zwischen LAN und WAN (Internet etc.) herstellen soll.

Aus diesem Grund implementiert man einen ISA Server 2004 als Firewall Lösung nicht in das interne Netzwerk – sprich, der ISA Server 2004 wird **KEIN** Mitglied der Domäne. Eine Ausnahme von der Regel ist ein ISA 2004 Server als reine Proxy Lösung. Dort befindet sich der ISA Server 2004 hinter einer anderen ISA 2004 Firewall oder Third Party Firewall und kann so Mitglied der Domäne sein, um z. B. über die integrierte Windows Authentifizierung ein Regelwerk für den Webzugriff abzubilden.

Die Benutzerseite

Stellen Sie sicher, dass die Benutzer eine RAS Einwahlberechtigung haben. Es handelt sich hierbei zwar um keine RAS Einwahl, aber mit diesem Schalter teilen Sie mit, dass jetzt RAS Richtlinien und IAS Richtlinien verwendet werden können, welche ja für den ISA Server 2004 Zugriff über RADIUS erforderlich sind.

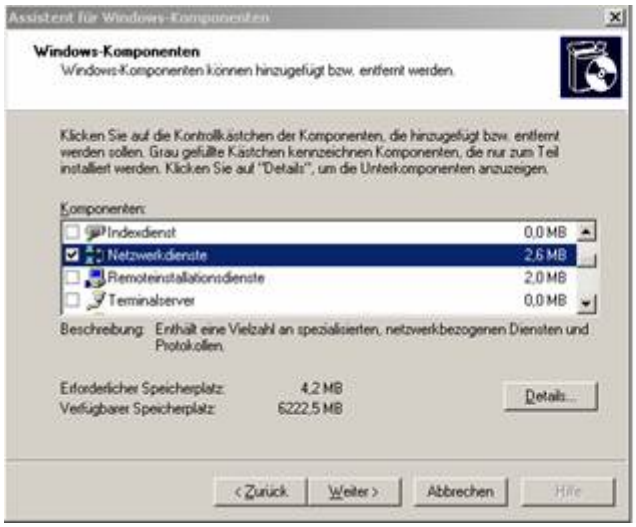
Müssen Sie mehreren Benutzern den Zugriff auf Dienste über den ISA ermöglichen, so empfiehlt sich das Anlegen einer Benutzergruppe um dieser die entsprechenden Berechtigungen zu vergeben und die entsprechenden Benutzer zum Mitglied dieser Gruppe zu machen.

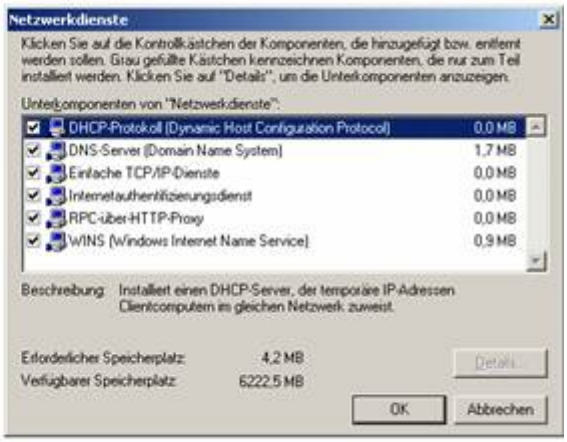
In unserem Beispiel verwenden wir die Gruppe *WWW-Benutzer*.

Installation der IAS Servers

Sie installieren den IAS Server wie jede Microsoft Komponente über Start – Systemsteuerung – Software – Windows Komponenten Hinzufügen / Entfernen.

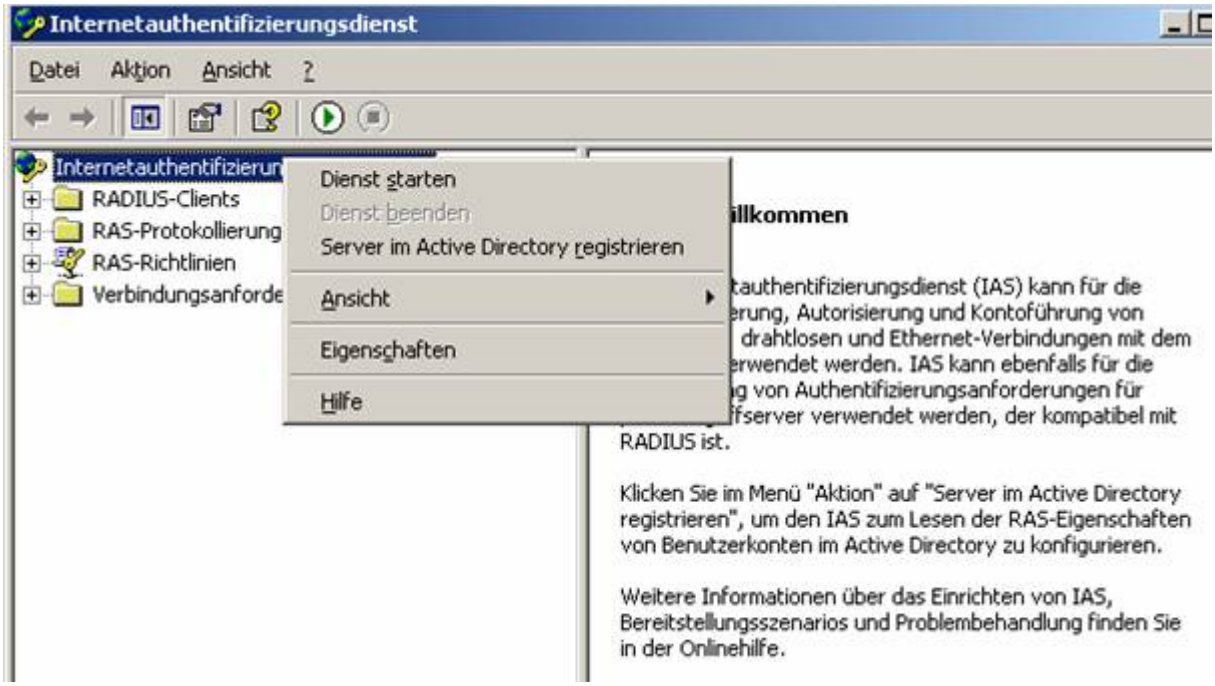
Gehen Sie dann in Netzwerkdienste und wählen dort *Internetauthentifizierungsdienst* aus.





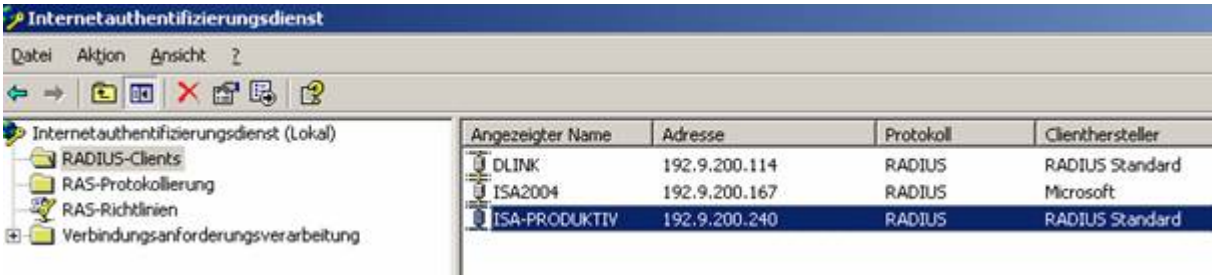
Nach erfolgter Installation des IAS müssen Sie diesen *Server im Active Directory registrieren*, damit der IAS berechtigt ist, Kontenanfragen über LDAP an das Active Directory zu richten.

Klicken Sie dazu in der IAS Konsole mit der rechten Maustaste auf *Internetauthentifizierungsdienst* und wählen im Kontextmenü *Server im Active Directory registrieren* aus.



Erstellen des ISA 2004 Servers als IAS Client

Damit der ISA Server 2004 eine Benutzerauthentifizierung über RADIUS nutzen kann, müssen Sie den ISA Server als RADIUS Client einrichten. Hierzu sind zwei Schritte erforderlich. Der erste Schritt ist es im IAS einen neuen RADIUS Client zu erstellen.Klicken Sie dazu mit de rechten Maustaste in den Container *RADIUS-Client* und fügen einen neuen Client hinzu.



Sie müssen einen Namen für den neuen RADIUS Client angeben. Das muss nicht zwingend der NetBIOS / DNS Name des Clients sein, es handelt sich hierbei nur um den angezeigten Namen.

Als nächstes müssen Sie die IP Adresse oder den DNS Namen des RADIUS Client angeben und den Clienthersteller auswählen. Wir wählen als Clienthersteller *RADIUS Standard*.

Ein sehr wichtiger Punkt ist das so genannte *Shared Secret* – beim IAS *Gemeinsam geheimer Schlüssel* genannt.

Hier bei handelt es sich um eine Methode der Authentifizierung zwischen ISA Server und IAS Client. Ist der gemeinsam geheime Schlüssel identisch, erfolgt eine Kommunikation zwischen Server und Client.

Es wird die Verwendung eines sehr langen und kryptischen Schlüssels empfohlen. Die Qualität steht und fällt mit der Länge und Komplexität des Schlüssels. Ein brauchbarer Schlüssel wäre zum Beispiel: Xd5$1“xSS(&aäsD03?Q.

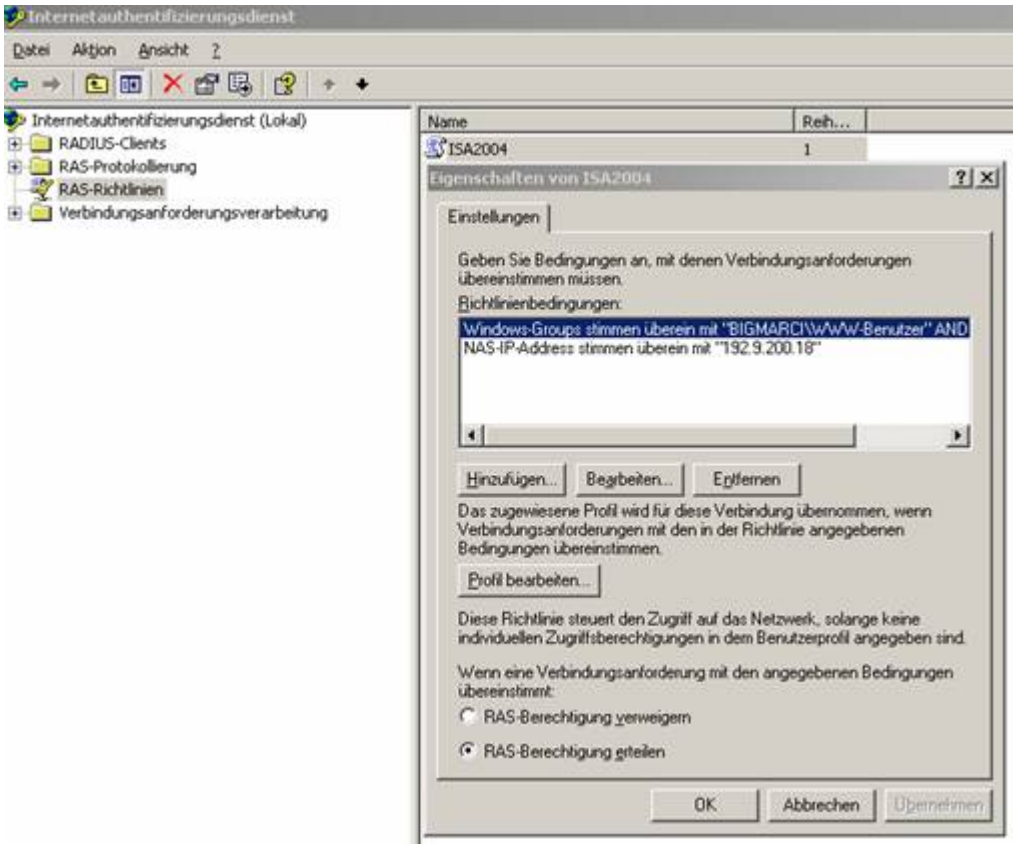
Wichtig:

Bei der Vergabe des geheimen Schlüssels ist die Groß- und Kleinschreibung zu beachten.

Den hier gewählten Schlüssel müssen Sie später auch noch beim ISA Server verwenden, also merken Sie sich den Schlüssel gut ☺

RAS Richtlinie

Erstellen Sie eine neue RAS-Richtlinie mit welcher Sie einer neu zu erstellen Active Directory Benutzergruppe *WWW-Benutzer* das Recht geben, den mit IP Adresse angegebenen ISA Server nutzen zu dürfen.



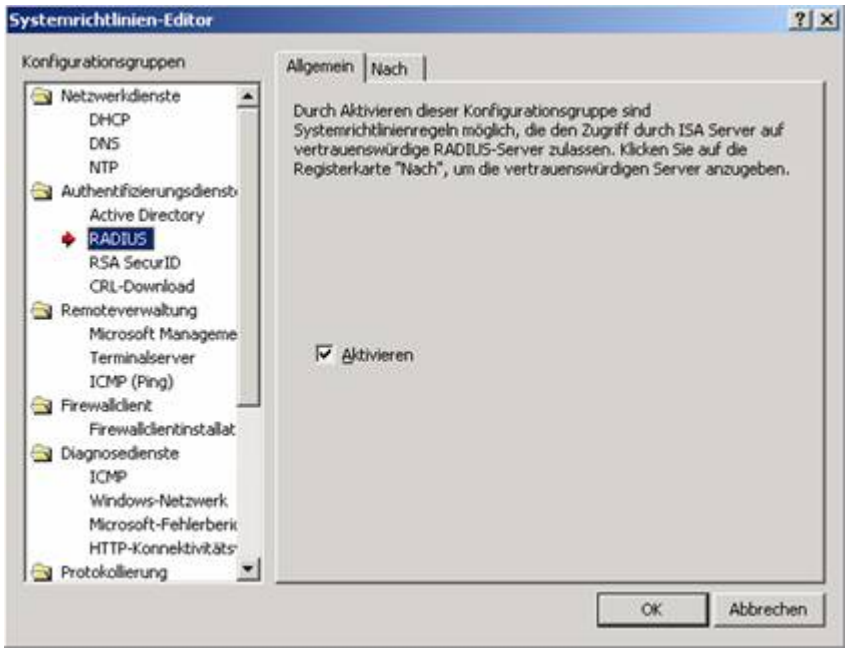
Auf dem ISA Server

Auf dem ISA Server 2004 müssen Sie verschiedene Konfigurationsänderungen vor nehmen, damit der ISA eine Benutzerauthentifizierung über IAS durchführt.

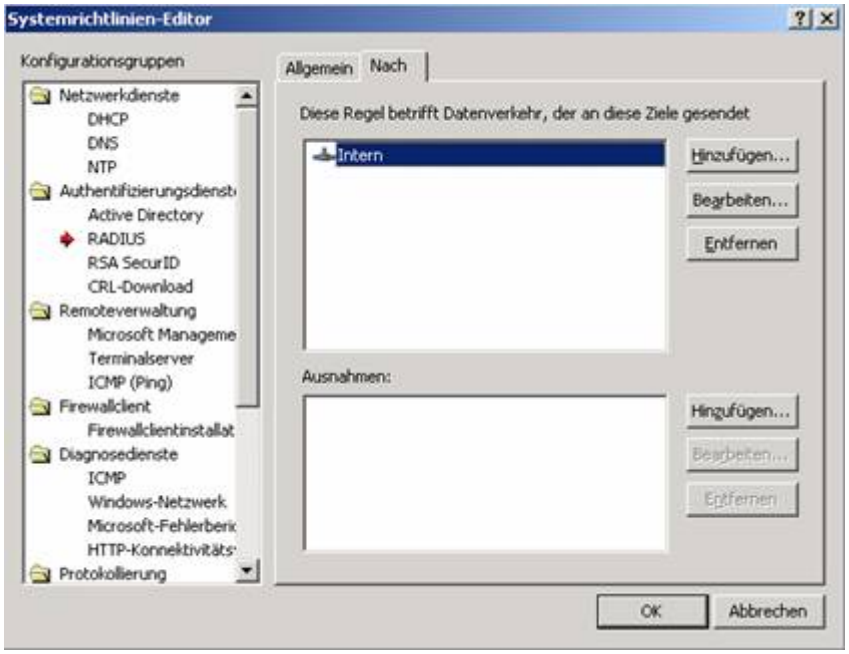
Als erstes müssen Sie überprüfen ob die ISA Server 2004 Firewall Systemrichtlinie den RADIUS Zugriff auf das interne Netzwerk zulässt.

Starten Sie dazu die ISA Server Verwaltungskonsole und klicken Sie mit der rechten Maustaste auf *Firewallrichtlinie* und wählen im Kontextmenü *Systemrichtlinie bearbeiten* aus.

Die Firewallrichtlinie ist per Default aktiviert …

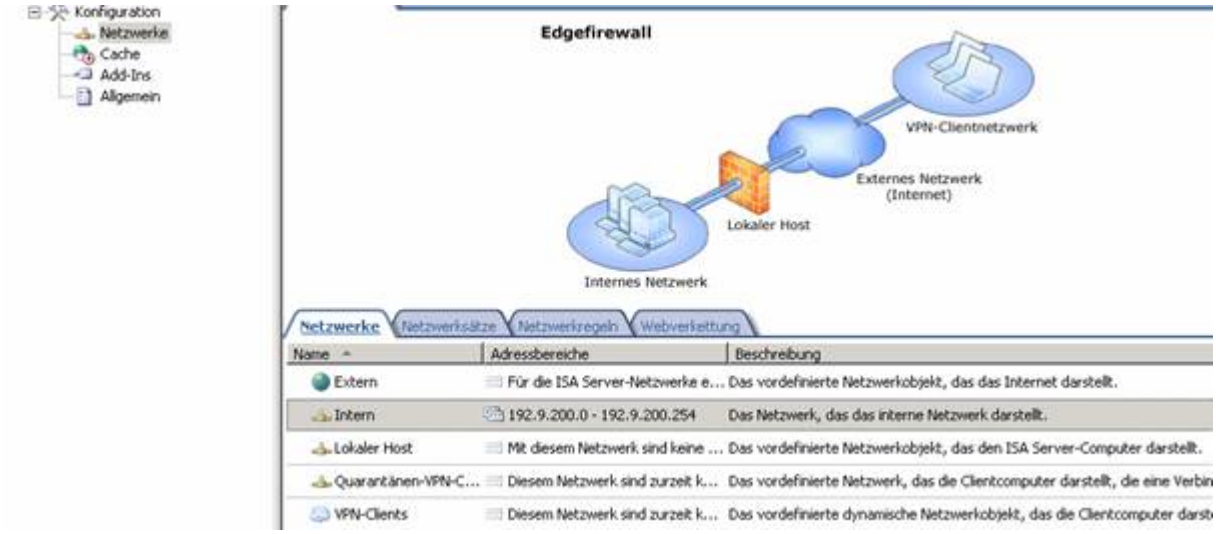


… mit Zugriff auf das Netzwerkobjekt *Intern*.



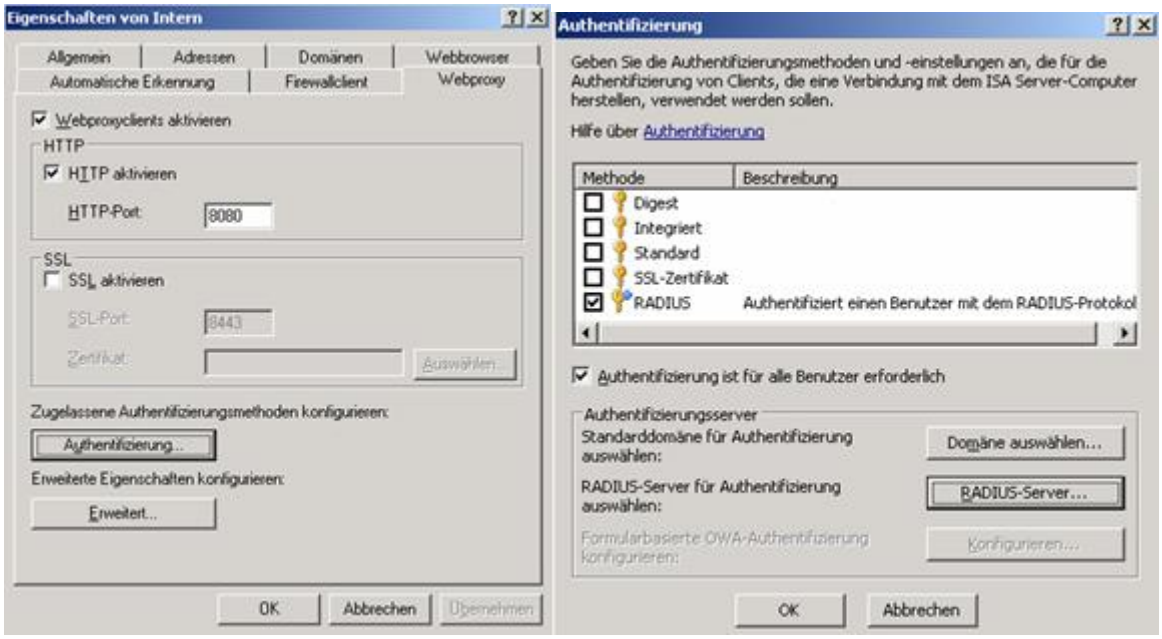
Als nächstes müssen wir dem Netzwerkobjekt *Intern* mitteilen, dass ab sofort eine Authentifizierung der Benutzer erfolgen muss und die Authentifizierungsmethode RADIUS ist.

Starten Sie dazu die ISA Verwaltungskonsole und navigieren Sie über die *Konfiguration* zum Container *Netwerke* und wählen dort das Netzwerkobjekt *Intern* aus und gehen in dessen Eigenschaften.



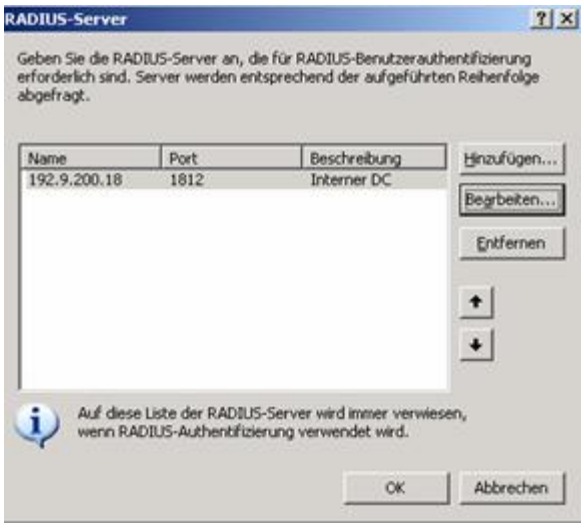
Klicken Sie auf den Reiter *Webproxy* und wählen dort bei der zugelassenen Authentifizierungsmethode *Authentifizierung* aus.

Im nun erscheinenden Fenster wählen Sie die Authentifizierungsmethode *Integriert* (Standardmethode) ab und klicken stattdessen auf *RADIUS*.

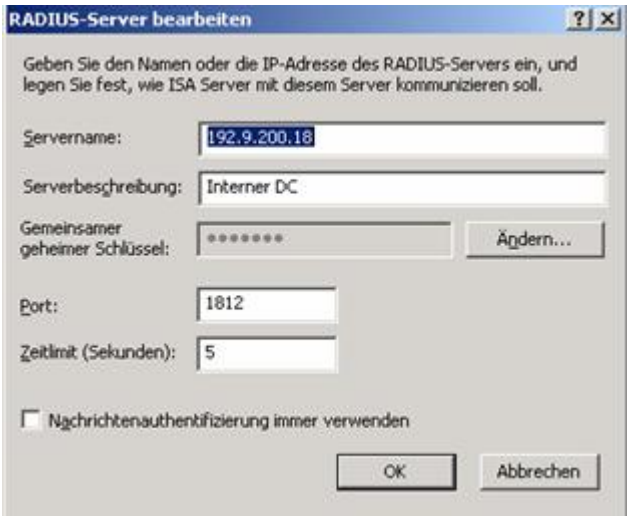


Als nächstes aktivieren Sie *Authentifizierung ist für alle Benutzer erforderlich*. Damit wird sichergestellt, dass nicht autorisierte Benutzer zur Authentifizierung aufgefordert werden.

Im Feld Authentifizierungsserver wählen Sie bitte *RADIUS-Server* aus. Es erscheint folgendes Fenster (in diesem Beispiel ist bereits ein RADIUS Server konfiguriert). Klicken Sie auf *Hinzufügen*.



Geben Sie unter Servername die IP Adresse oder den Namen des IAS Servers an. Die Serverbeschreibung ist optional, jedoch zur besseren Orientierung und zur Dokumentation sinnvoll.



Im Feld *Gemeinsamer geheimer Schlüssel* geben Sie den im IAS erstellen Schlüssel an. Sie erinnern sich: Xd5$1“xSS(&aäsD03?Q. Bestätigen Sie den Schlüssel noch einmal.

Tipp: *Verwenden Sie* ***NICHT*** *den Schlüssel aus diesem Beispiel.*

Der Standard *Port* für RADIUS ist 1812,1645 für die Authentifizierung und 1813,1646 für die Kontoführung. Ändern Sie die Ports nicht. Wenn ja, müssen die Änderungen auch am IAS erfolgen.

Das *Zeitlimit (Sekunden)* sollten Sie nur verändern, wenn der ISA Probleme hat in dieser Zeit den IAS zu kontaktieren. Das sollte aber nur sehr selten bis gar nicht der Fall sein.

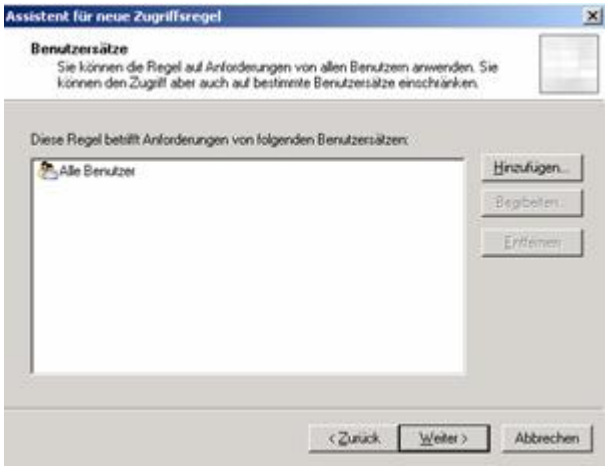
Den Punkt *Nachrichtenauthentifizierung immer verwenden* können Sie unverändert lassen.

Firewallregel auf dem ISA Server

Der nächste Schritt ist die Erstellung eine Firewallrichtlinie mit der Verwendung von RADIUS als Benutzerauthentifizierung. In diesem Beispiel verwenden wir eine Firewallrichtlinie für den HTPP/HTTPS Zugriff für einen Active Directory Benutzer namens MSISAFAQ.

Die ersten Schritte des Assistenten zur Erstellung einer Firewallrichtlinie erspare ich mir, weil diese sich nicht von der Erstellung einer normalen Regel unterscheiden.

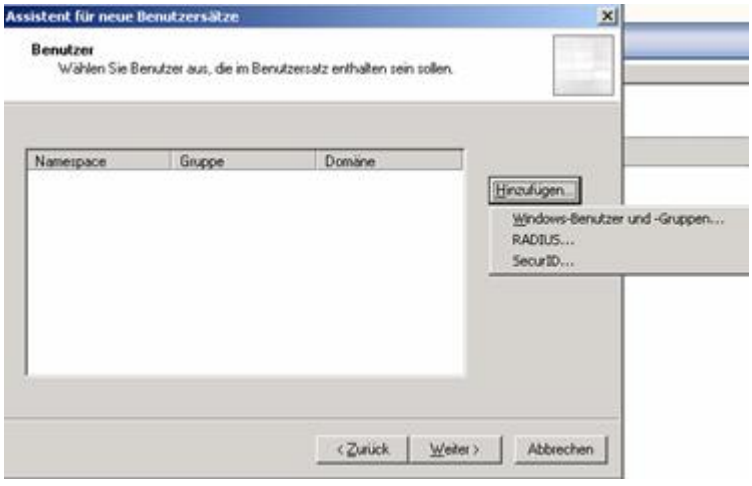
Wir steigen bei dem Punkt *Benutzersätze* des Assistenten für neue Zugriffregeln ein. Entfernen Sie *Alle Benutzer* und klicken Sie auf *Hinzufügen* um einen neuen Benutzersatz zu erstellen.



Klicken Sie auf *Neu*

Im Assistenten für Benutzersätze vergeben Sie einen Namen für den neuen Benutzersatz.

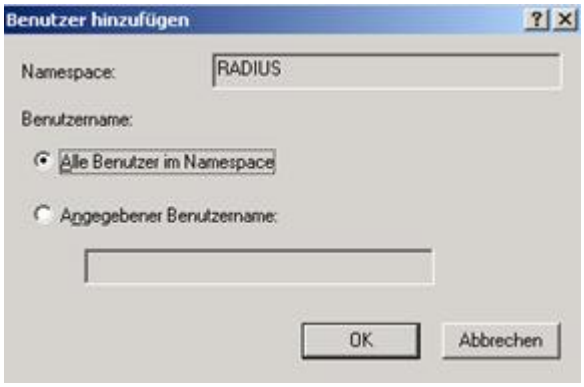
Im Fenster *Benutzer* klicken Sie auf *Hinzufügen* und wählen *RADIUS* aus.



Der Namespace ist RADIUS.

Als Benutzername stehen zur Wahl:

- Alle Benutzer im Namespace – entspricht der Gruppe JEDER der Active Directory Domäne
- Angegebener Benutzername – entspricht dem Active Directory Benutzernamen.



Wir wählen *Alle Benutzer im Namespace*

Das Regelwerk ist fast fertig. Wählen Sie jetzt noch den neu erstellten Benutzersatz aus und bestätigen Sie die neu erstellte Firewallrichtlinie.

Sie können diese Regel jetzt verwenden um dem Benutzer das Surfen über den ISA Server 2004 zu erlauben.

Hinweis: *Ein weiterer interessanter Anwendungszweck einer Authentifizierung über RADIUS ist VPN. Ohne RADIUS muss der ISA Server, der gleichzeitig als VPN Server konfiguriert ist, zwingend Domänenmitglied sein. Mittels RADIUS kann der ISA auch als alleinstehender Server konfiguriert sein.*

SMTP-Anwendungsfilter

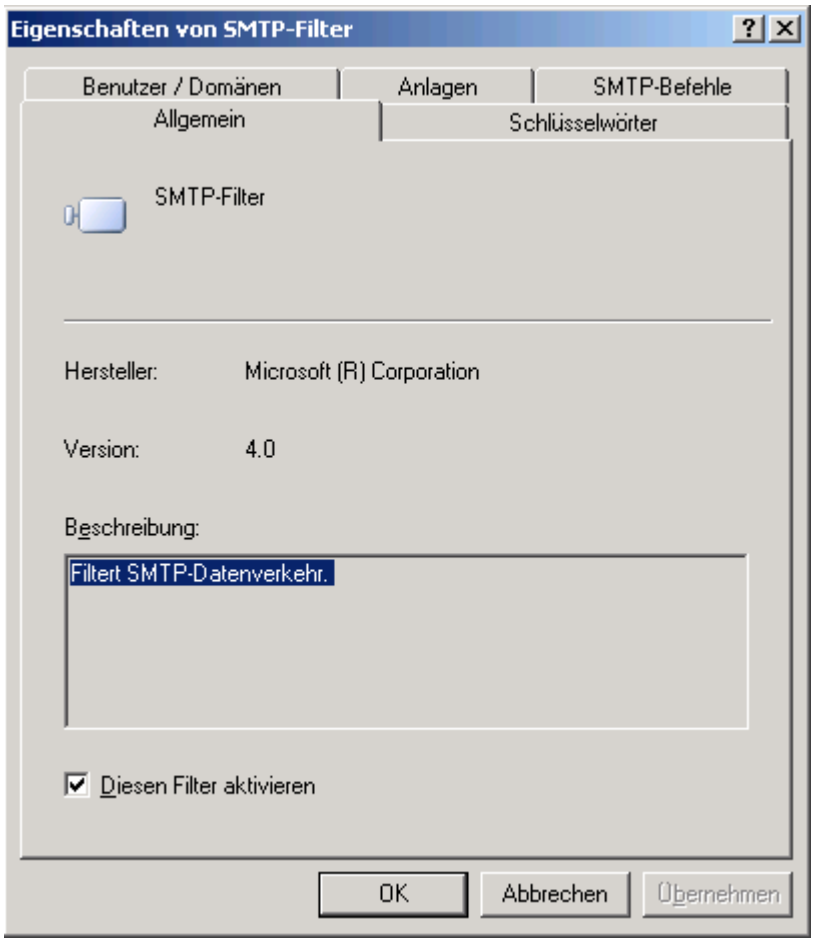
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

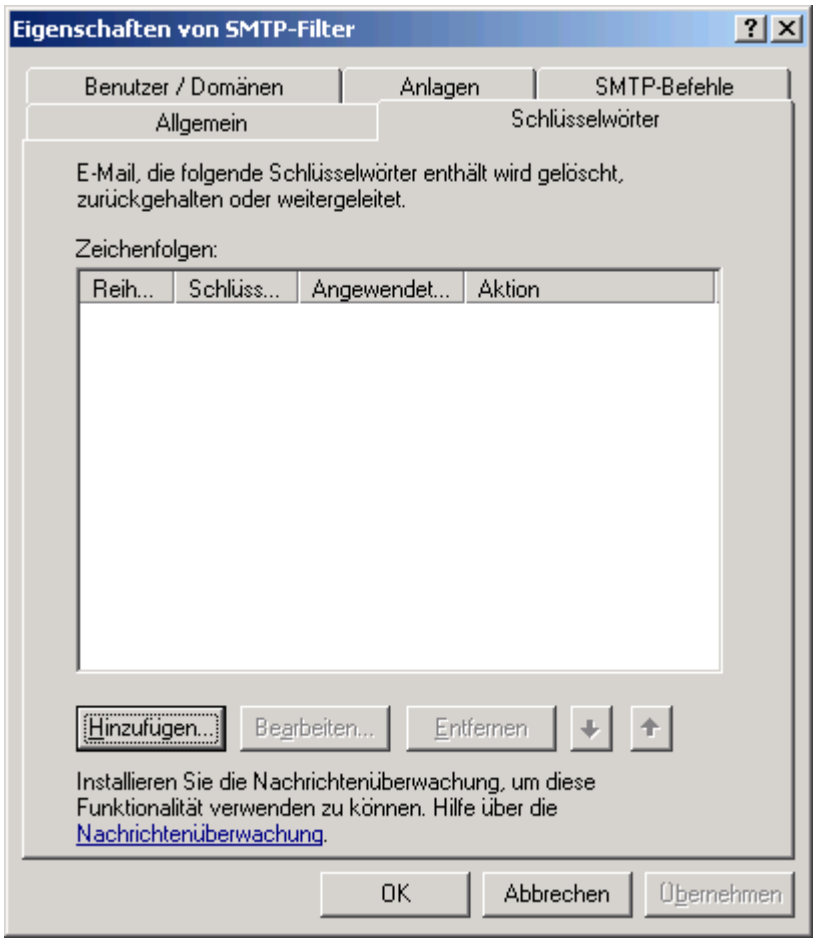
Der ISA Server filtert standardmäßig sämtlichen SMTP-Verkehr, der an Port 25 des ISA Server-Computers eintrifft. Der SMTP-Filter übernimmt den Datenverkehr, untersucht ihn, und leitet ihn nur dann weiter, wenn die Regeln dies zulassen. Der SMTP-Filter kann mit der Nachrichtenüberwachung zusammenarbeiten, um eine intensivere Untersuchung des Inhalts zu gewährleisten. Die Nachrichtenüberwachung muss gesondert installiert und konfiguriert werden, was in diesem Artikel nicht beschrieben wird. Der vorliegende Artikel möchte kurz die einfachste Schutzmöglichkeiten dieses Filters beschreiben.

Der SMTP-Filter überprüft die von Internet-SMTP-Servern und -Clients gesendeten SMTP-Befehle. Der Filter ist in der Lage, SMTP-Befehle abzufangen und zu überprüfen, ob sie länger als erlaubt sind. SMTP-Befehle, die größer als die festgelegten Grenzwerte sind, werden als Angriffe auf den SMTP-Server aufgefasst und können vom SMTP-Filter abgewehrt werden. Jeder SMTP-Befehl besitzt eine festgelegte maximale Länge. Diese Länge entspricht der Anzahl Bytes, die für jeden Befehl zulässig sind. Wenn ein Angreifer einen Befehl sendet, dessen Länge die Anzahl der für diesen Befehl zulässigen Bytes überschreitet, unterbricht ISA Server die Verbindung und verhindert so den Datenaustausch zwischen dem Angreifer und dem Mailserver des Unternehmens. Wenn ein Client einen Befehl verwendet, der zwar definiert aber deaktiviert ist, beendet der Filter die Verbindung. Gleiches gilt für einen Befehl, der nicht definiert ist. Im Fall eines Verstoßes gegen den SMTP-Filter kann ein Alarmereignis erzeugt werden, worauf vordefinierte Aktionen ausgeführt werden können.

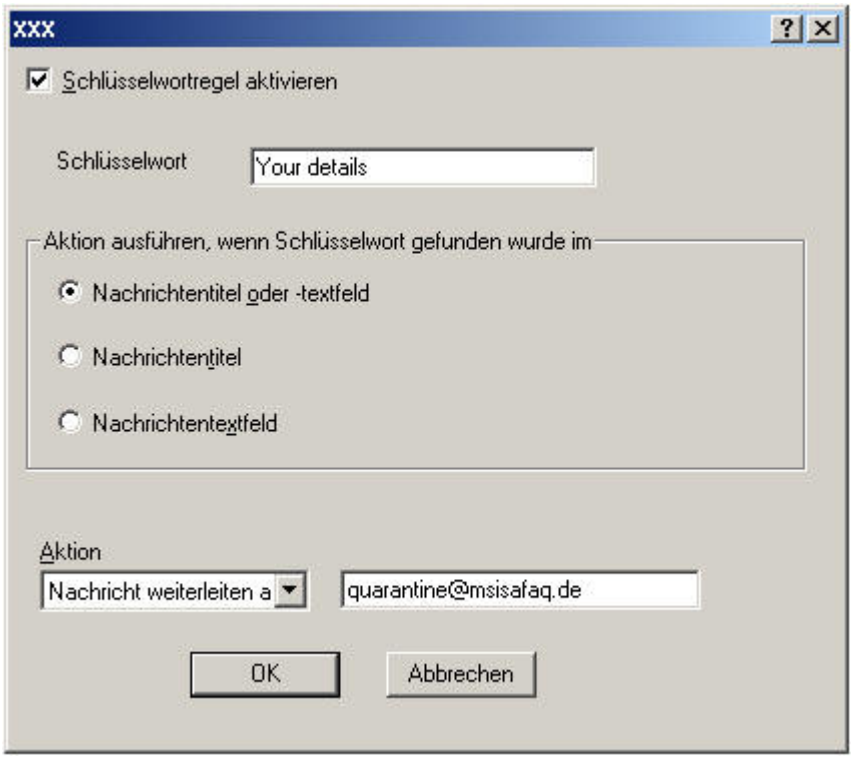
Der SMTP Filter hat in der Grundeinstellung folgende Registerkarten:



Im Gegensatz zum ISA Server 2000 ist in der aktuellen Version der SMTP Filter nach der Installation aktiviert.

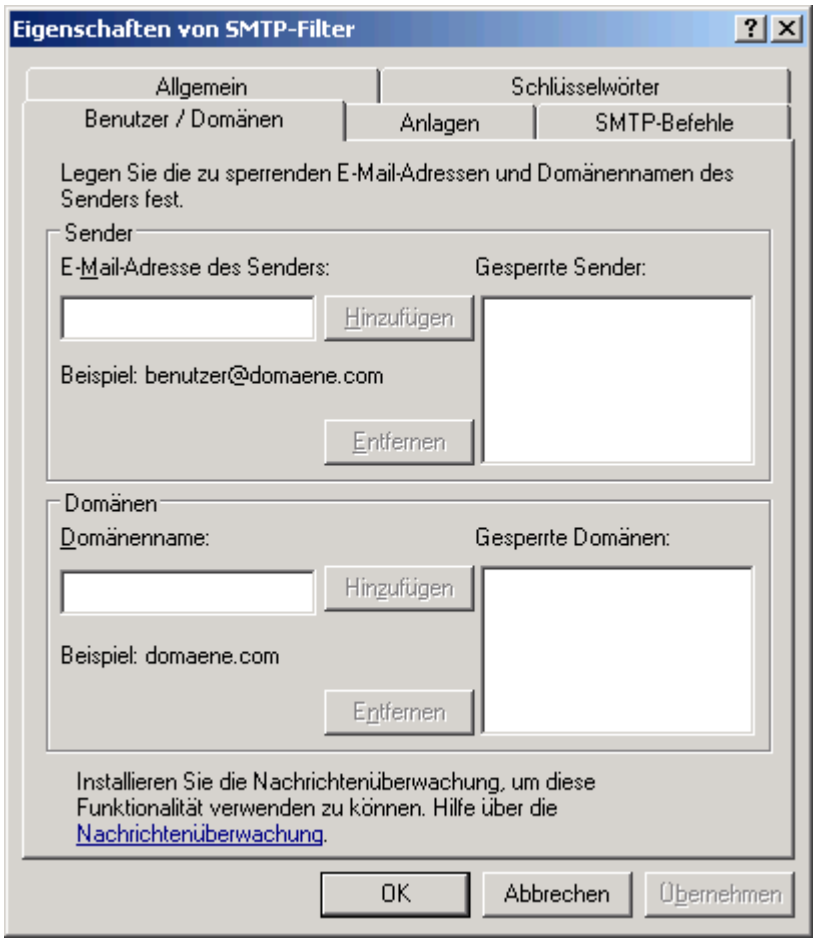


Wenn die Nachrichtenüberwachung konfiguriert wurde, können an dieser Stelle bestimmte Schlüsselworte gefiltert werden:

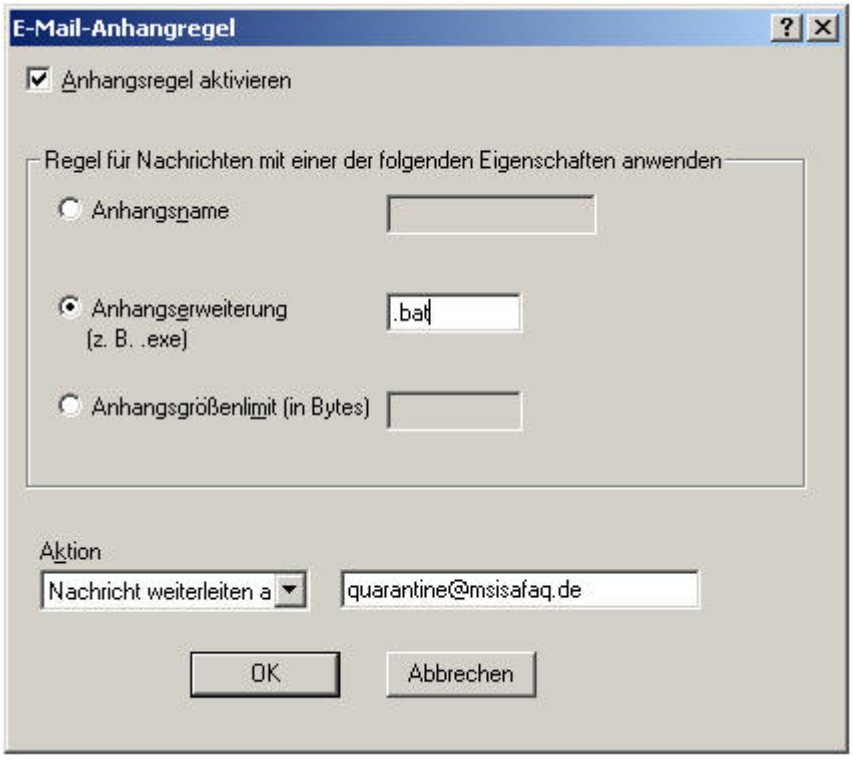


Unter "Aktion" stehen folgende Möglichkeiten zur Verfügung:

- Nachricht löschen: Die Nachricht wird verworfen
- Nachricht halten: Die Nachricht landet im Badmail-Verzeichnis
- Nachricht weiterleiten an: hier muss eine Adresse eingegeben werden, an die die Nachricht weitergeleitet werden soll



An dieser Stelle können Anlagen blockiert werden:



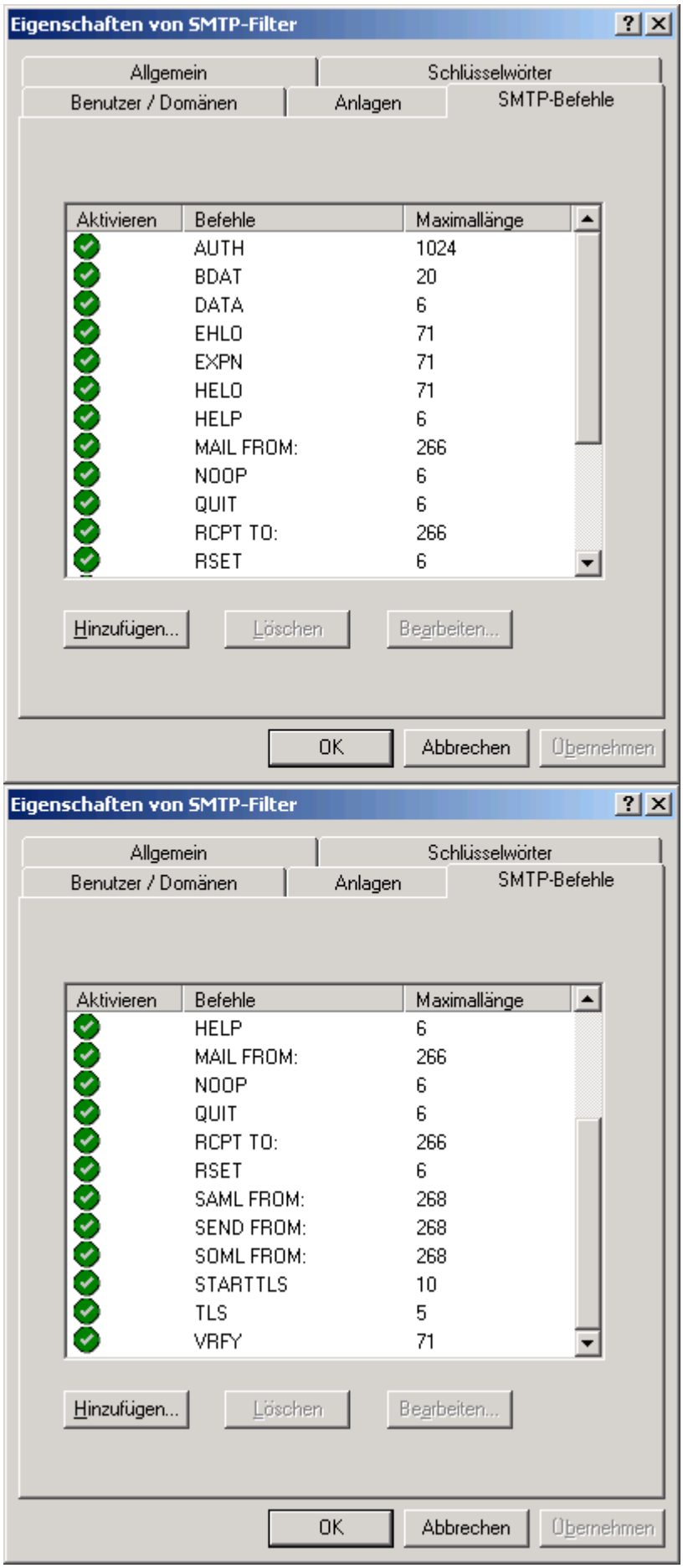
Unter "Aktion" stehen wieder die drei Möglichkeiten zur Verfügung:

- Nachricht löschen: Die Nachricht wird verworfen
- Nachricht halten: Die Nachricht landet im Badmail-Verzeichnis
- Nachricht weiterleiten an: hier muss eine Adresse eingegeben werden, an die die Nachricht weitergeleitet werden soll

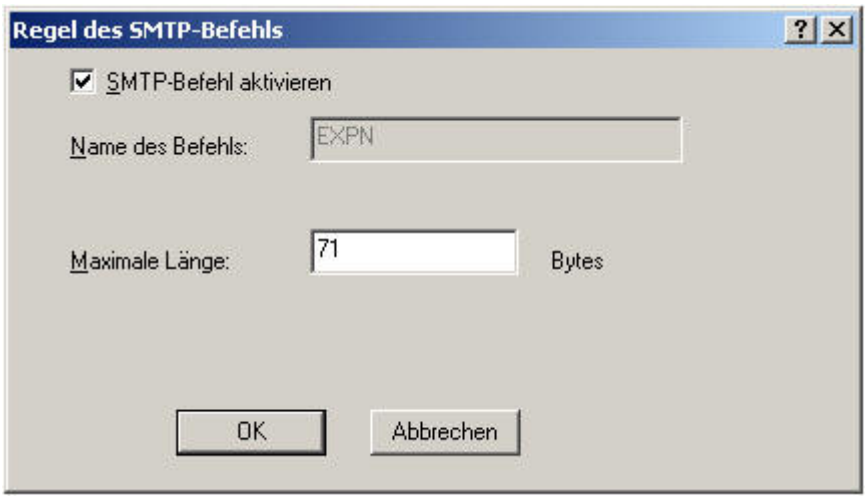
Ich empfehle meistens, geblockte Mails nicht zu löschen sondern an ein speziell überwachtes (und auf Viren geprüftes!) Postfach weiterzuleiten. Somit geht keine Mail verloren, was je nach Einsatzzweck in einem Unternehmen wichtig sein könnte. Es ist immer ein Abwägungsspiel, welche Anlagen gesperrt werden sollen. Einerseits soll möglichst eine hohe Sicherheit erreicht werden, andererseits sollen die Anwender möglichst wenig in ihrer täglichen Arbeit behindert werden.

Folgende Anlagen sind prinzipiell als gefährlich einzustufen:

.acm	Windows Systemdatei	.msi	Windows Installationsdatei
.bas	Visual Basic Klassenmodul	.msp	Windows Installationsdatei
.bat	Batchfile	.mst	Visual Source Datei
.bin	Binärdatei	.ocx	OLE Steuerungsdatei
.chm	Kompilierte Hilfe-Datei	.otm	VBA Projekt Datei
.cmd	Windows Kommandoscript	.ov*	Programm Overlay Datei
.com	Ausführbare Datei	.pif	DOS-Programminformation
.cla	Java Applet	.pl	Pearl Script
.class	Java Applet	.reg	Registrierungsdatenbankdatei
.cpl	Systemsteuerungsanwendung	.scr	Bildschirmschoner
.crt	Zertifikat	.scf	Explorer Kommandodatei
.drv	Gerätetreiber	.sct	Windows Scriptingkomponente
.exe	Ausführbare Datei	.shb	Document Scrap Objekt
.fon	Schriftart	.shs	Shell Scrap Objekt
.fot	Schriftart	.sys	Systemdatei
.dll	Dynamische Link Library	.tlb	Typ Bibliothek
.hta	HTML Anwendung	.url	Internetverknüpfung
.ini	Einstellungsdatei	.vb	VBScript Datei
.inf	Installationsdatei	.vbe	VBScript Encoded Datei
.ins	Internetkommunikationseinstellungen	.vbs	VBScript Datei
.isp	Internetkommunikationseinstellungen	.v*d	Virtueller Gerätetreiber
.js	JScript Datei	.ws	Windows Scriptingdatei
.jse	JScripe Encoded Datei	.wsc	Windows Scripting Komponente
.lnk	Verknüpfung (Shortcut)	.wsf	Windows Scriptingdatei
.mpd	Miniport Gerätetreiber	.wsh	Windows Scripting Einstellungen


Eigenschaften von SMTP-Filter
Allgemein
Schlüsselwörter
Benutzer / Domänen
Anlagen
SMTP-Befehle
Aktivieren
Befehle
Maximallänge
AUTH 1024
BDAT 20
DATA 6
EHLO 71
EXPN 71
HELO 71
HELP 6
MAIL FROM: 266
NOOP 6
QUIT 6
RCPT TO: 266
RSET 6
Hinzufügen...
Löschen
Bearbeiten...
OK
Abbrechen
Übernehmen
Eigenschaften von SMTP-Filter
Allgemein
Schlüsselwörter
Benutzer / Domänen
Anlagen
SMTP-Befehle
Aktivieren
Befehle
Maximallänge
HELP 6
MAIL FROM: 266
NOOP 6
QUIT 6
RCPT TO: 266
RSET 6
SAML FROM: 268
SEND FROM: 268
SOML FROM: 268
STARTTLS 10
TLS 5
VRFY 71
Hinzufügen...
Löschen
Bearbeiten...
OK
Abbrechen
Übernehmen

In der Registerkarte "SMTP-Befehle" können (und sollten) verschiedene Befehle gesperrt bzw. zugelassen werden, die bei der Kommunikation zwischen Mailservern benötigt werden. Dies ist die einzige Sperrmöglichkeit, die ohne Installation und Konfiguration der Nachrichtenüberwachung zur Verfügung steht und daher genutzt werden sollte. Sämtliche SMTP Befehle, die hier nicht eingetragen sind werden vom ISA Server geblockt, sobald der SMTP Filter aktiviert ist. Dies ist auch der Grund, warum er direkt nach der Installation deaktiviert ist. Neben den zugelassenen Befehlen kann auch die maximale Länge der Befehlsoptionen festgelegt werden, um einen Pufferüberlauf zu verhindern.



Die meisten Befehle benötigen nur eine bestimmte Anzahl an nachfolgenden Optionen, sodass dies keine Operative Einschränkung ist. Z.B. ist für das Kommando "Mail from:" eine Länge von 266 Zeichen vorkonfiguriert. Dies reicht sicherlich aus, um die komplizierteste Absendemailadresse abzubilden, denn welche Mailadresse hat mehr als 266 Zeichen? Möglicherweise hat aber der interne SMTP Server ein Sicherheitsloch, was ausgenutzt werden könnte, wenn man ihm Mailadressen mit 2000 Zeichen übergibt. Um dem vorzubeugen, setzt der ISA Server mit seinem SMTP Filter eine Beschränkung.

Bestehende vorkonfigurierte Befehle können nicht gelöscht werden, sie können nur deaktiviert werden. Es ist problemlos möglich, neue Befehle hinzuzufügen (diese können dann auch wieder gelöscht werden).

Es empfiehlt sich, gefährliche oder nicht-benötigte Befehle prinzipiell zu sperren:

- EXPN: Das EXPN (Expand) Kommando erweitert eine Verteilerliste, sodass der Absender alle in der Verteilerliste enthaltenen Mailadressen herausbekommen kann.
- NOOP: Der NOOP (NO Operation) Befehl ist für den funktionalen Betrieb überflüssig. Er bewegt den Mailserver lediglich dazu, eine OK-Statusmeldung zu liefern. Im übertragenen Sinn ist er mit dem ping-Befehl vergleichbar.
- VRFY: Das VRFY (verify) Kommando wird dazu benutzt um einen Benutzernamen beim Mailserver zu überprüfen.

Hinweis: Wenn ein Client den TURN-Befehl verwendet, werden alle entsprechenden E-Mails vom Filter aussortiert.

Hinweis: Laut RFC ist der AUTH-Befehl Bestandteil des MAIL FROM-Befehls. Aus diesem Grund sperrt der SMTP-Filter MAIL FROM-Befehle nur, wenn sie die zulässige Länge der MAIL FROM- und AUTH-Befehle überschreiten (wenn AUTH aktiviert ist). Wenn Sie zum Beispiel für MAIL FROM eine maximale Länge von 266 Bytes und für AUTH eine Länge von 1024 Bytes festlegen, wird die Nachricht nur gesperrt, wenn der MAIL FROM-Befehl 1290 Bytes übersteigt.

Hinweis: Ich möchte nochmals betonen, dass ohne installierter und konfigurierter Nachrichtenüberwachung lediglich die Registerkarte "Befehle" Wirkung zeigt.

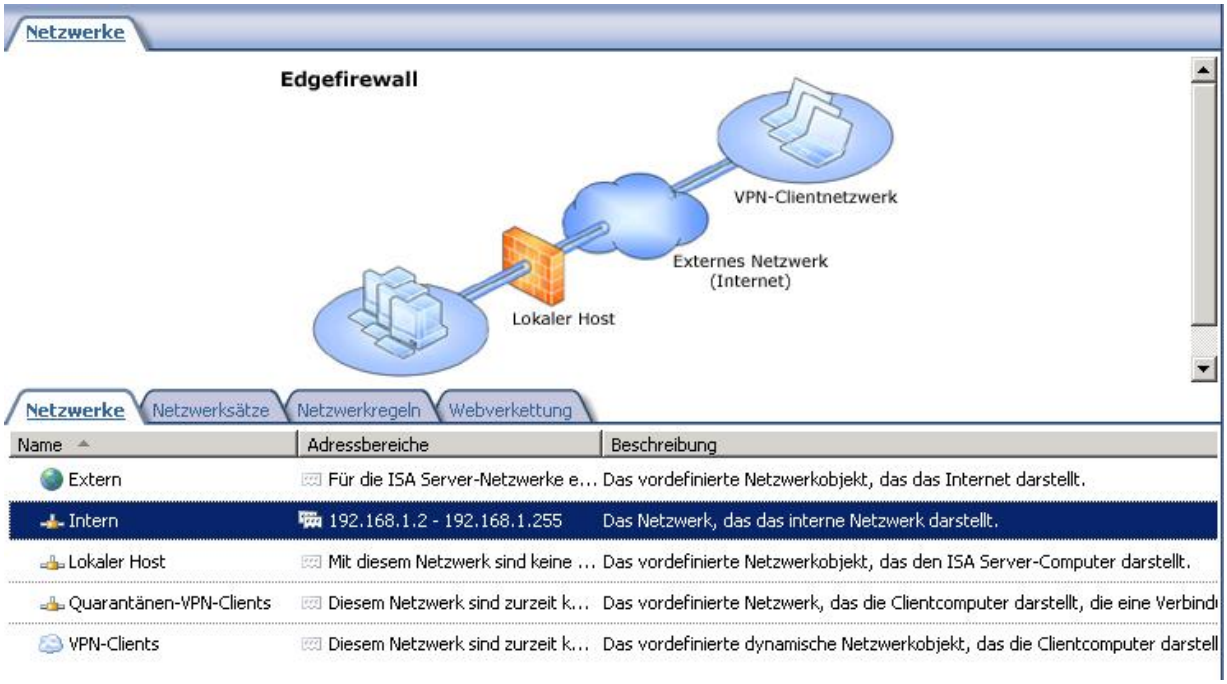
Erstellen eines neuen Netzwerkes

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

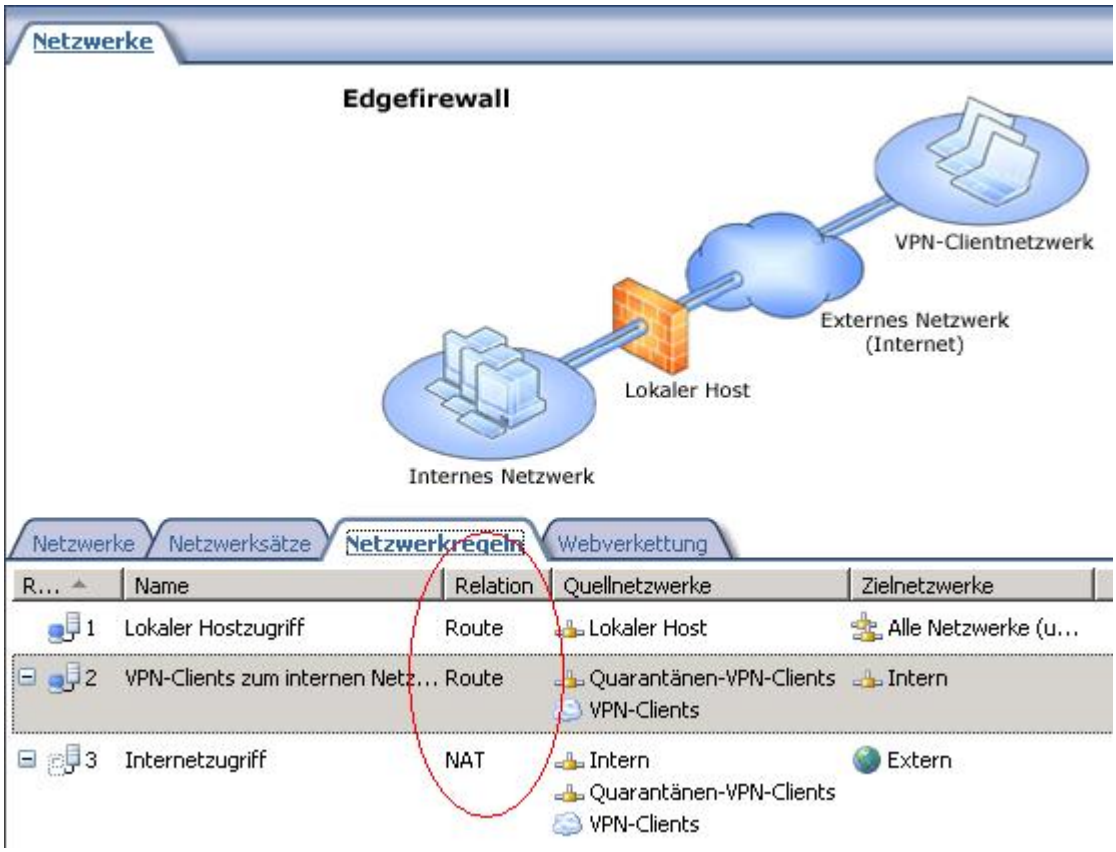
Microsoft ISA Server 2004 bietet als erste Microsoft Firewall die Möglichkeit, mehrere Netzwerkobjekte zu definieren und diese Netzwerkobjekte mit beliebigen anderen Netzwerkobjekten in Beziehung zu setzen.



Diese Netzwerke können vom ISA Administrator in eine ...

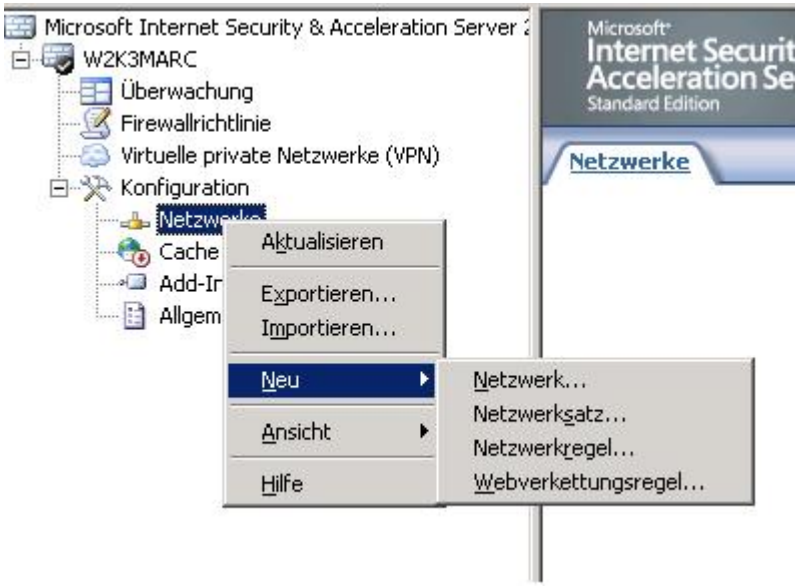
- NAT (Network Address Translation) oder
- ROUTE

Beziehung zu einander gesetzt werden.

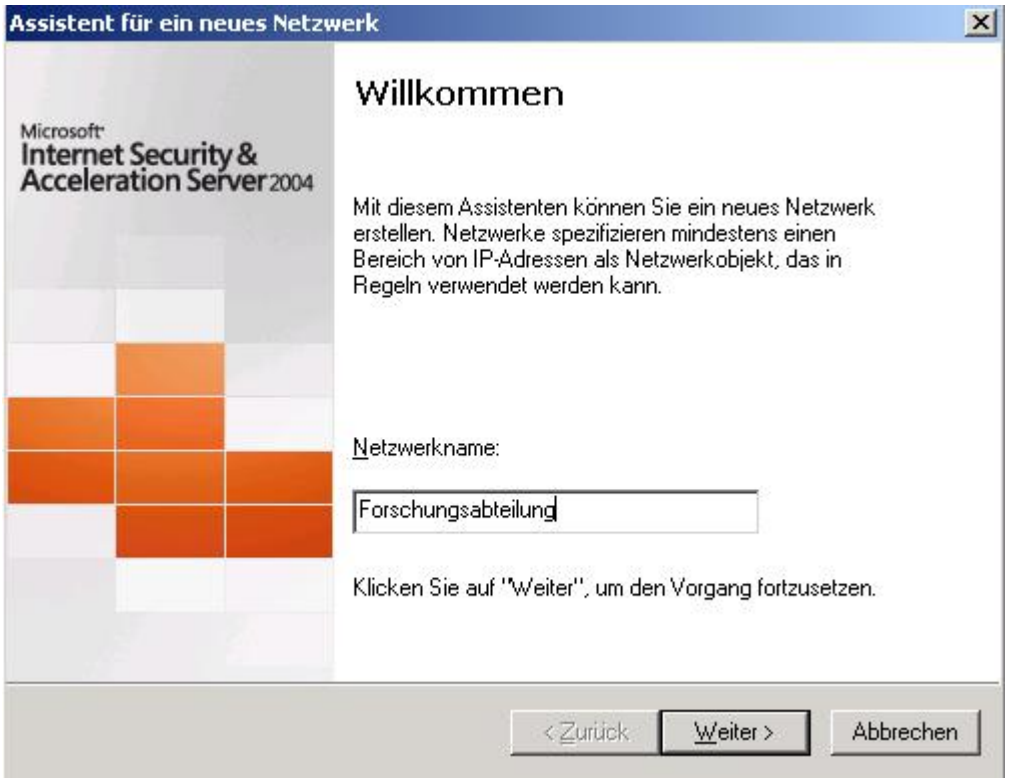


Dieser Artikel beschreibt die Erstellung eines neuen Netzwerkes mit dem Ziel für die Forschungsabteilung, welche sich in einem eigenen IP-Subnetz befindet, ein neues Netzwerk anzulegen, und den PCs in diesem Netzwerk den Zugriff auf Ressourcen im Internet zu ermöglichen.

Starten Sie die ISA Server Verwaltungskonsole und klicken Sie mit der rechten Maustaste unterhalb von ***Konfiguration*** auf ***Netzwerke***. Klicken Sie im Kontextmenü auf ***Netzwerk***, um ein neues Netzwerk zu erstellen.



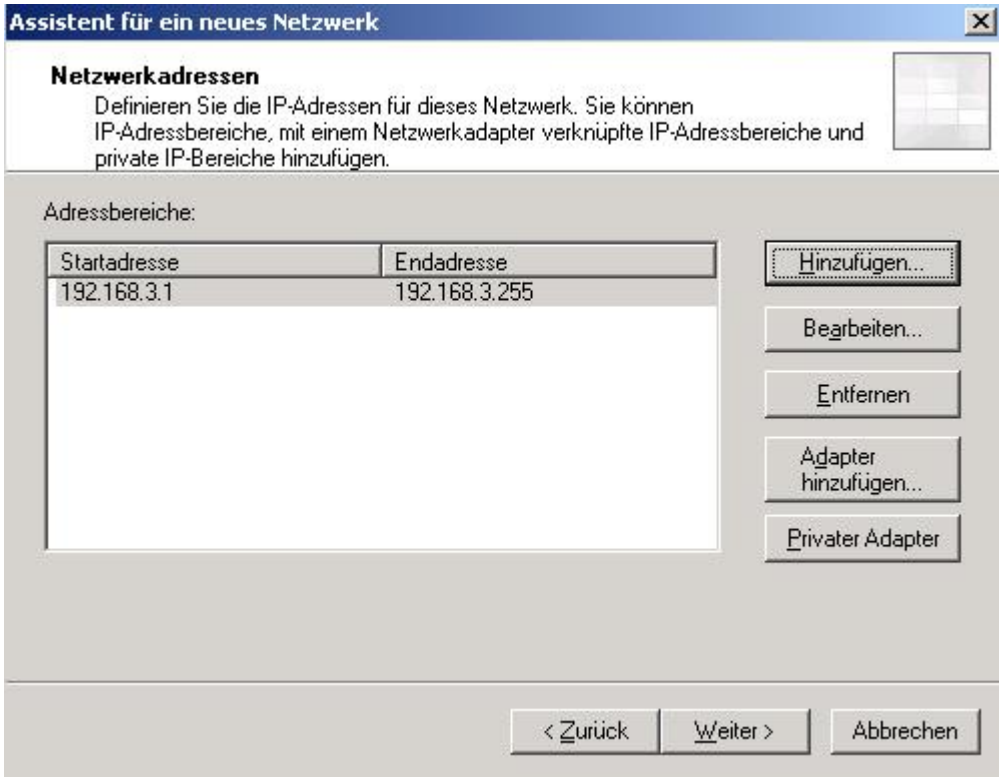
Geben Sie dem neuen Netzwerk einen Namen.



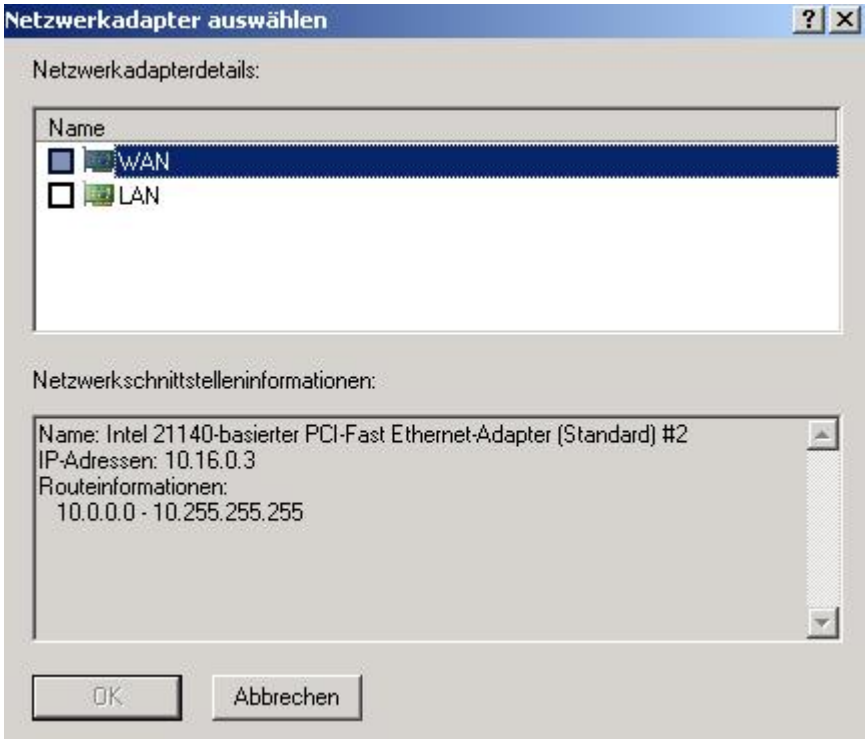
Geben Sie jetzt den Typ des zu erstellenden Netzwerkes an. Wir wählen in unserem Beispiel ***Internes Netzwerk***.

Die Bedeutung der Netzwerke ist selbsterklärend. Es sei hier nur ein Hinweis auf die Bedeutung des Umkreisnetzerk gegeben.
Als Umkreisnetzwerk bezeichnet man auch die DMZ = DeMilitarisierte Zone. Der Begriff DMZ sollte den meisten Lesern geläufiger sein.

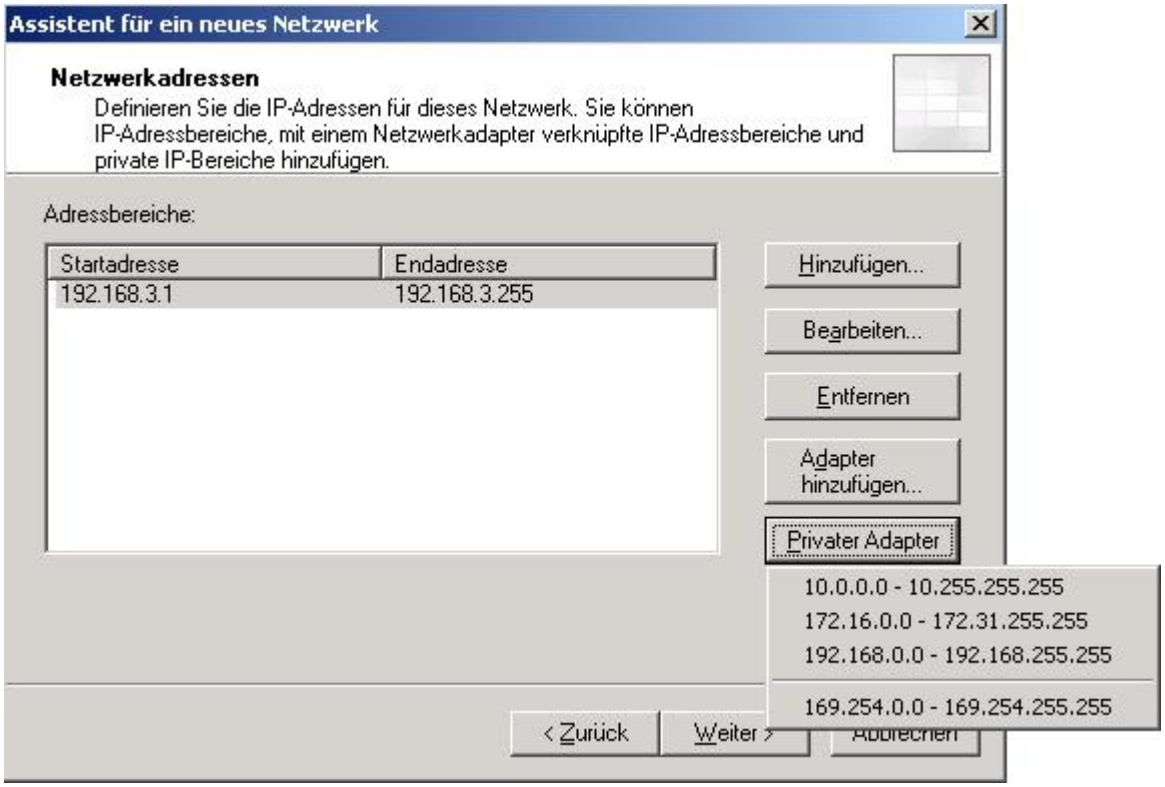
Geben Sie jetzt einen IP-Adressbereich für das neue Netzwerk an. in diesem Beispiel wählen wir den Netzwerkbereich ***192.168.3.1 - 192.168.3.255*** .



Sie können auch einen Netzwerkadapter auswählen, aus dem der ISA Server Assistent den neuen Netzwerkbereich erstellen soll. Klicken Sie dazu auf ***Adapter hinzufügen***.



Haben Sie INTERN einen Standard Netzwerkbereich aus den privaten Netzwerken der Klasse A / B und C, können Sie hier auch auf ***Privater Adapter*** klicken und den Netzwerkbereich hinzufügen.



Der Assistent hat alle Informationen, welche er zur Erstellung des Netzwerkes benötigt, gesammelt und zeigt Ihnen diese Informationen in einer Zusammenfassung an. Klicken Sie unbedingt auf ***Hilfe über weitere Konfigurationsschritte***, denn noch ist die Konfiguration nicht vollständig.

Schritte zur Netzwerkkonfiguration

Damit neu erstellte Netzwerke Datenverkehr senden oder empfangen können, müssen weitere Konfigurationsschritte durchgeführt werden. Diese Schritte sind vom Typ des erstellten Netzwerks abhängig.

Internes, externes und Umkreisnetzwerk

Damit Clients in diesen Netzwerken Datenverkehr senden und empfangen können, müssen Sie die folgenden Schritte durchführen:
Erstellen Sie eine Netzwerkregel, die Datenverkehr zu und von diesem Netzwerk zulässt. Entsprechende Anweisungen finden Sie unter Erstellen einer Netzwerkregel.

Erstellen Sie Firewallrichtlinienregeln, die Datenverkehr zu und von diesem Netzwerk zulassen. Entsprechende Anweisungen finden Sie unter Erstellen einer Zugriffsregel, Erstellen einer Webveröffentlichungsregel, Erstellen einer Serververöffentlichungsregel oder Veröffentlichen eines Mailservers.

Standort-zu-Standort-VPN mit IPSec

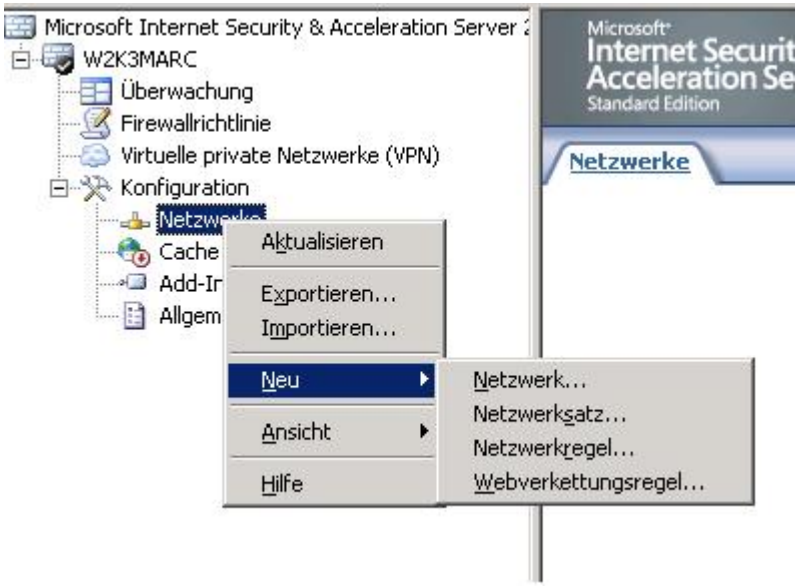
Damit Clients Verbindungen aus einem VPN (Virtual Private Network) mit IPSec (Internet Protocol Security) herstellen können, müssen Sie folgende Schritte durchführen:
Erstellen Sie eine Netzwerkregel, die Datenverkehr zu und von diesem Netzwerk zulässt.
Erstellen Sie Zugriffsregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.
Überprüfen Sie die IPSec-Protokolleinstellungen mithilfe der Eigenschaften des neu erstellten Netzwerks.

Standort-zu-Standort-VPN mit PPTP oder L2TP

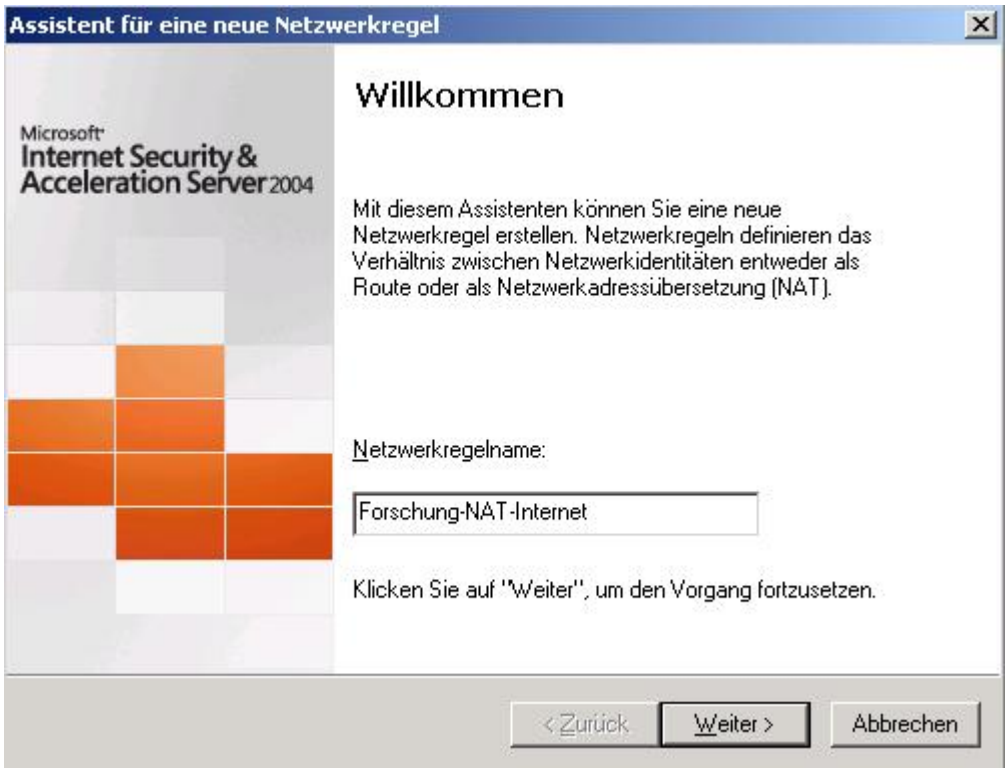
Damit Clients eine Verbindung aus dem VPN über PPTP (Point-to-Point Tunneling-Protokoll) oder L2TP (Layer Two Tunneling-Protokoll) herstellen können, müssen Sie die folgenden Schritte durchführen:
Erstellen Sie einen Benutzer mit dem Namen des neuen Netzwerks. Geben Sie dann für die RAS-Berechtigungen Zulassen an. Entsprechende Anweisungen finden Sie unter Erstellen von Benutzern und Gruppen für Remote-VPN-Clients.
Erstellen Sie Netzwerkregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.
Erstellen Sie Zugriffsregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.

Klicken Sie in der ISA Verwaltungskonsole unterhalb von ***Konfiguration*** auf ***Netzwerke*** und überprüfen Sie im Reiter ***Netzwerke*** , ob das entsprechende Netzwerk korrekt erstellt wurde.

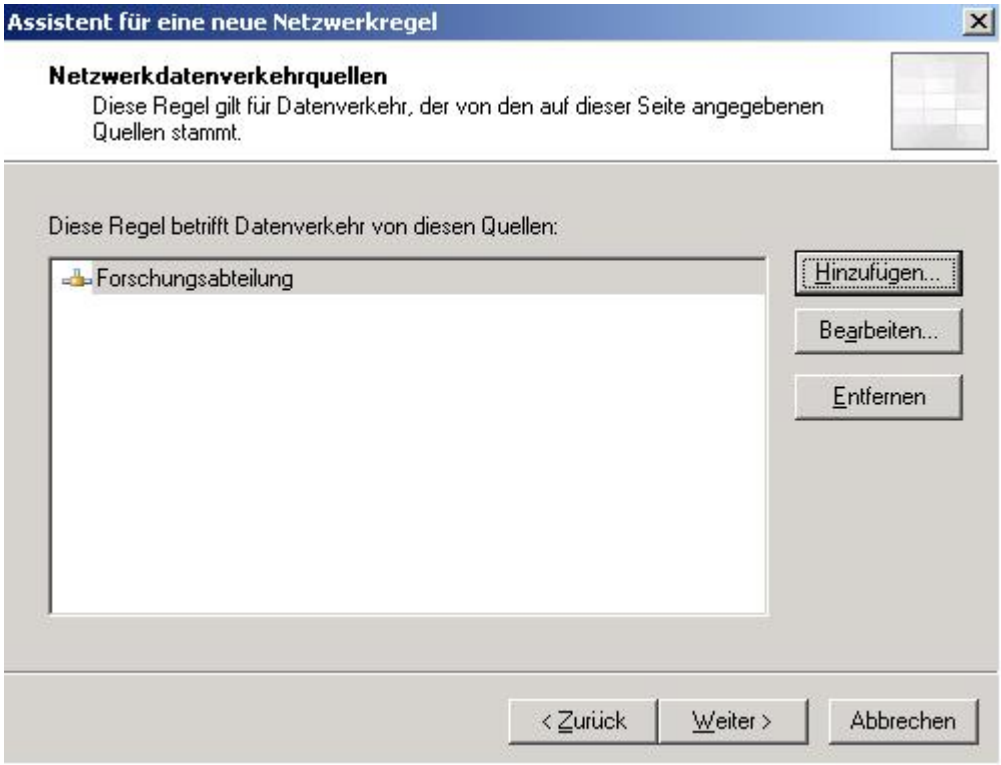
Im nächsten Schritt ist die Erstellung einer Netzwerkregel notwendig. Mit Hilfe der Netzwerkregel regeln Sie wie das neue Netzwerk mit dem Zielnetzwerk kommunizieren soll.



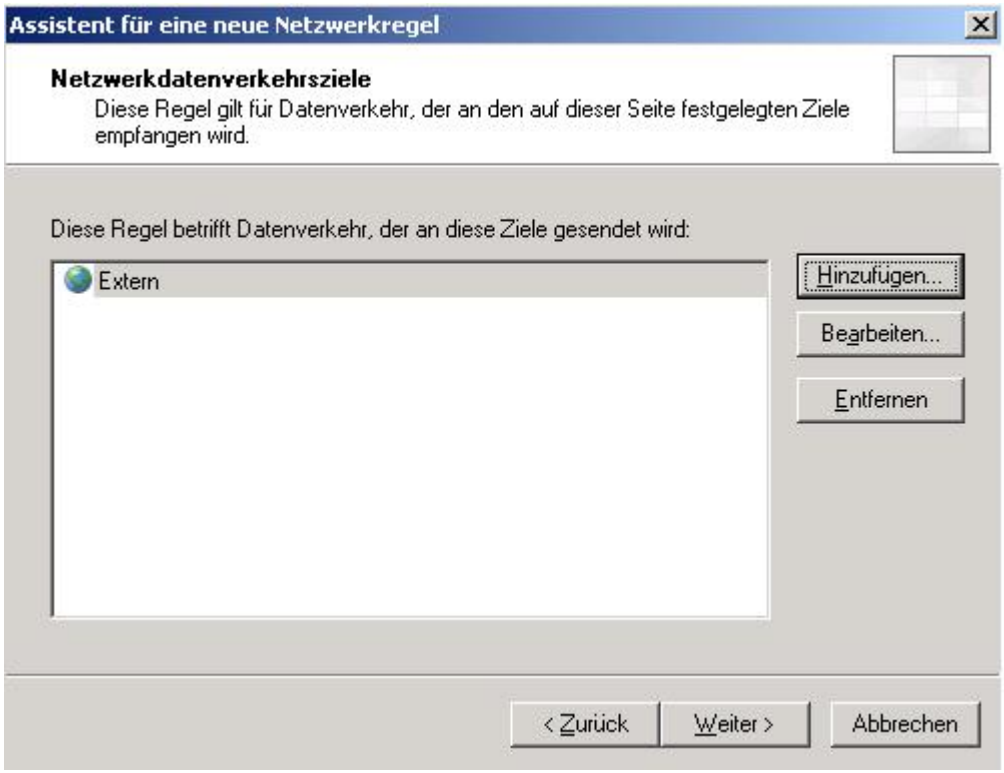
Geben Sie der Netzwerkregel einen sprechenden Namen.



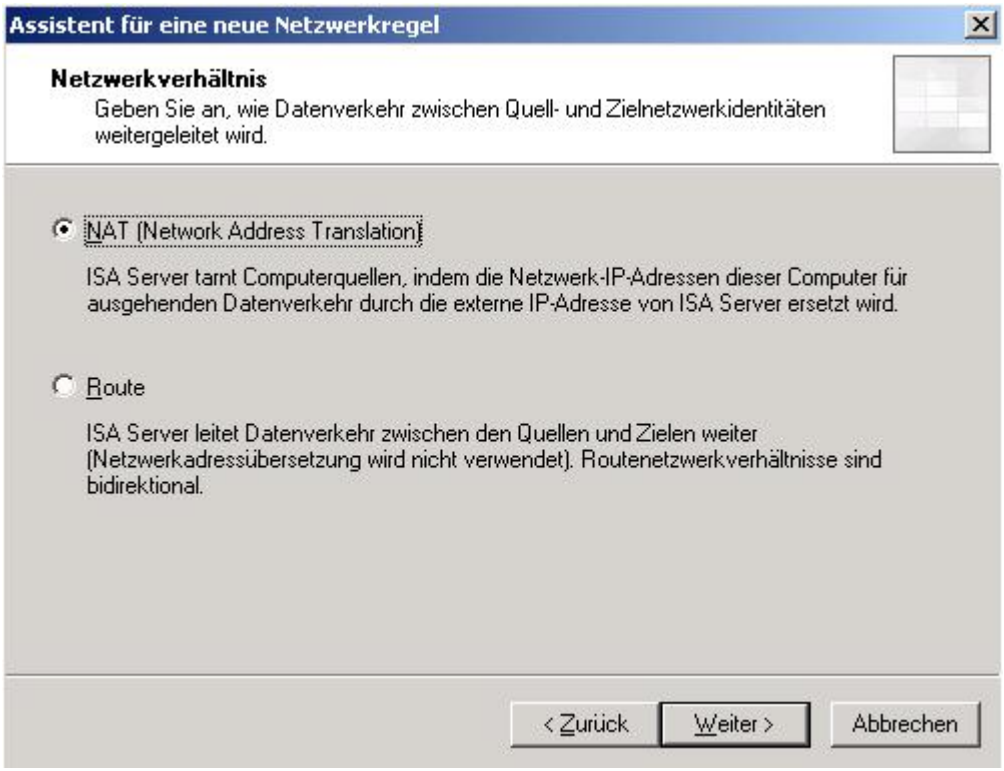
Netzwerkdatenverkerkehrquelle ist das Netzwerk ***Forschungsabteilung***.



Das Netzwerkdatenverkehrsziel ist ***Extern*** , da eine Internet Verbindung hergestellt werden soll.



Das Netzwerkverhältnis ist ***NAT (Network Address Translation).*** Mit Hilfe von NAT maskiert der ISA Server die IP-Adressen der internen Clients mit der externen IP Adresse des ISA Servers.



Klicken Sie in der ISA Verwaltungskonsole unterhalb von ***Konfiguration*** auf ***Netzwerke*** und überprüfen Sie im Reiter ***Netzwerkregeln***, ob die entsprechende Netzwerkregel korrekt erstellt wurde.

Der letzte Schritt ist die Erstellung eine Firewallrichtlinie für das neu erstellte Netzwerk.

Die neue Firewallrichtlinie soll den ***HTTP/HTTPS*** Zugriff für das Netzwerk ***Forschungsabteilung*** nach ***Extern*** für A***lle Benutzer*** zulassen.

ISA Server 2004 – Erstellen einer Webverkettung (Proxy-Chain)

Die Informationen in diesem Artikel beziehen sich auf:

Microsoft ISA Server 2004

Einleitung

In größeren Firmenumgebungen mit Zweigstellen kommt es häufiger vor, dass in der Zweigstelle ein ISA Server 2004 als Firewall oder Webproxy konfiguriert ist und dieser über den zentralen ISA Server 2004 in der Firmenzentrale eine Verbindung zum Internet herstellt. Diese Art der Anbindung von mehreren Proxy Servern über eine Kaskadierung an das Internet wird als Webverkettung bzw. Proxy Chaining bezeichnet.

Gründe für eine Webverkettung könnten sein:

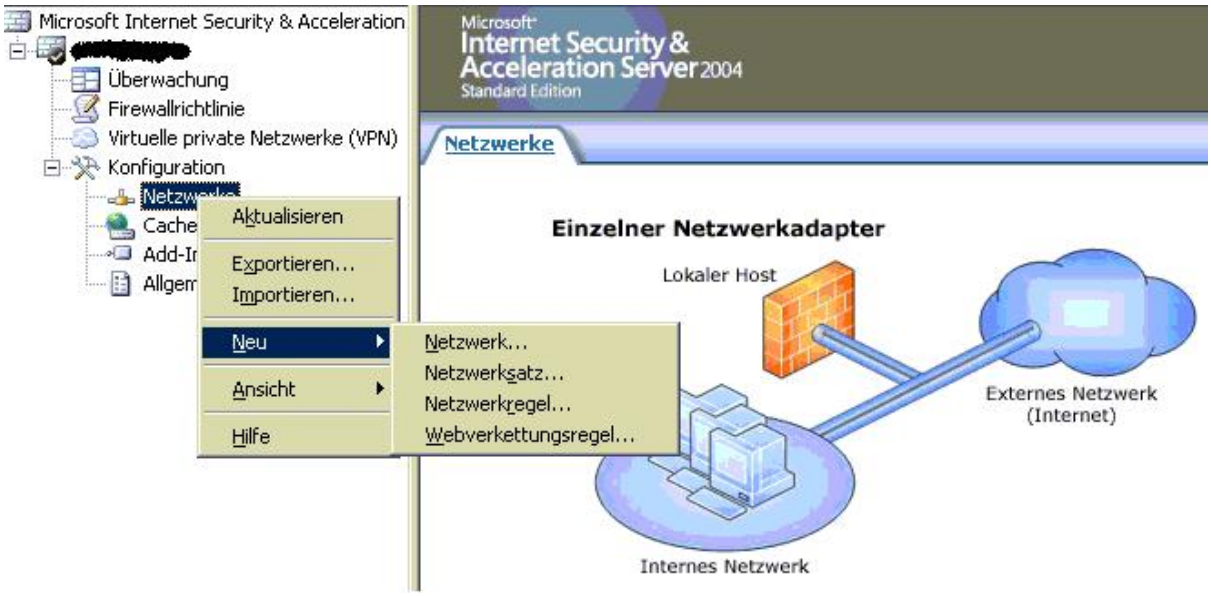
- Ein zentraler Internetzugang aus Sicherheitsgründen, aber Nutzung der Proxy Funktionalitäten zur Reduzierung der Netzwerklast zwischen den Zweigstellen und der Firmenzentrale
- Kaskadierung mit einem weiteren Proxy Server z. B. mit einem Proxy Server eines Rechenzentrums wenn der Firma

Bemerkung:

Eine Webverkettung kann auch zwischen einem ISA Server und einem ***NICHT*** ISA Server hergestellt werden, eine Firewallverkettung hingegen kann ***NUR*** mit ISA Servern durchgeführt werden.

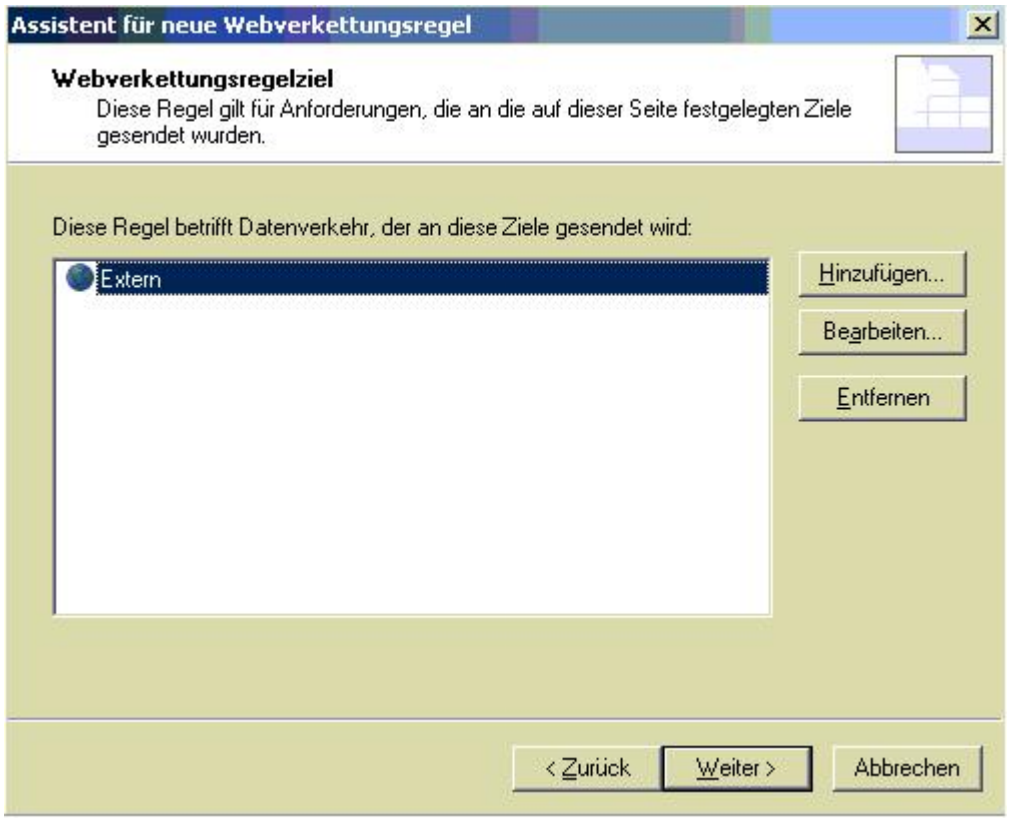
Dieser Artikel beschreibt die Einrichtung einer Webverkettung zwischen einem ISA Server 2004 in einer Zweigstelle und der Firmenzentrale.

Zur Konfiguration der Webverkettung starten Sie die ISA Server Verwaltungskonsole, erweitern den Container ***Konfiguration*** und klicken mit der rechten Maustaste auf ***Netzwerke***. Wählen Sie aus dem Kontextmenü ***Webverkettungsregel*** aus und folgen Sie den Anweisungen des Wizards.



Vergeben Sie einen sinnvollen Namen für die Webverkettungsregel. In diesem Beispiel verwenden wir den Namen ***ISA-Ausstenstelle zu ISA-Firmenzentrale***.

Geben Sie im Fenster ***Webverkettungsregel*** das Ziel für den Datenverkehr an. Da in diesem Beispiel eine Internetverbindung hergestellt werden soll, wählen wir das Netzwerkobjekt ***EXTERN*** aus.



Im Fenster ***Aktion anfordern*** können Sie die Anforderungsverarbeitung konfigurieren. Routingregeln legen fest, ob die Anforderung eines Webproxyclients direkt abgerufen, an einen anderen Upstreamproxyserver oder an ein anderes Ziel gesendet werden sollen.

Anforderungen direkt vom angegebenen Ziel abrufen

Gibt an, dass ISA Server Anforderungen von Webproxyclients direkt an das Internet sendet.

Anforderungen an angegebenen Upstreamserver weiterleiten

Gibt an, dass ISA Server Anforderungen von Webproxyclients zur Verarbeitung an einen Upstreamserver sendet. Der Upstreamserver entscheidet dann, ob die Anforderung zugelassen oder abgewiesen wird.

Delegierung der Anmeldeinformationen für Basisauthentifizierung zulassen

Lässt die Authentifizierung des Clients durch den Webserver zu, an den die Anforderung weitergeleitet wird. Wie der Name vermuten lässt, wird hier nur die Weitergabe der Credentials einer Basisauthentifizierung durchgeführt.

Einstellungen für Upstreamserver

Klicken Sie auf Einstellungen, um den Upstreamserver zu konfigurieren, der die Anforderungen bearbeitet.

Alternativroute

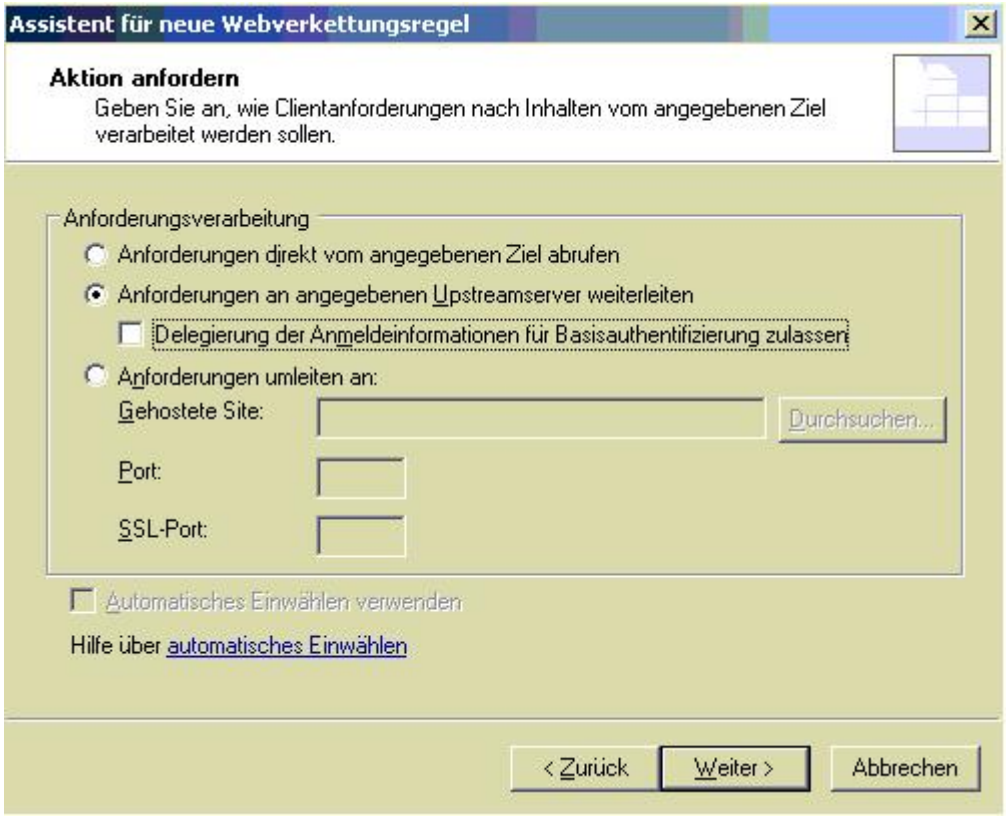
Listet optionale ISA Server-Computer zum Bearbeiten von Anforderungen auf, wenn die Primärroute nicht verfügbar ist. Wenn Sie Upstreamproxyserver auswählen, müssen Sie festlegen, welcher Server verwendet wird.
Klicken Sie auf Einstellungen, um den für die Alternativroute verwendeten Upstreamserver zu konfigurieren.

Anforderungen umleiten an

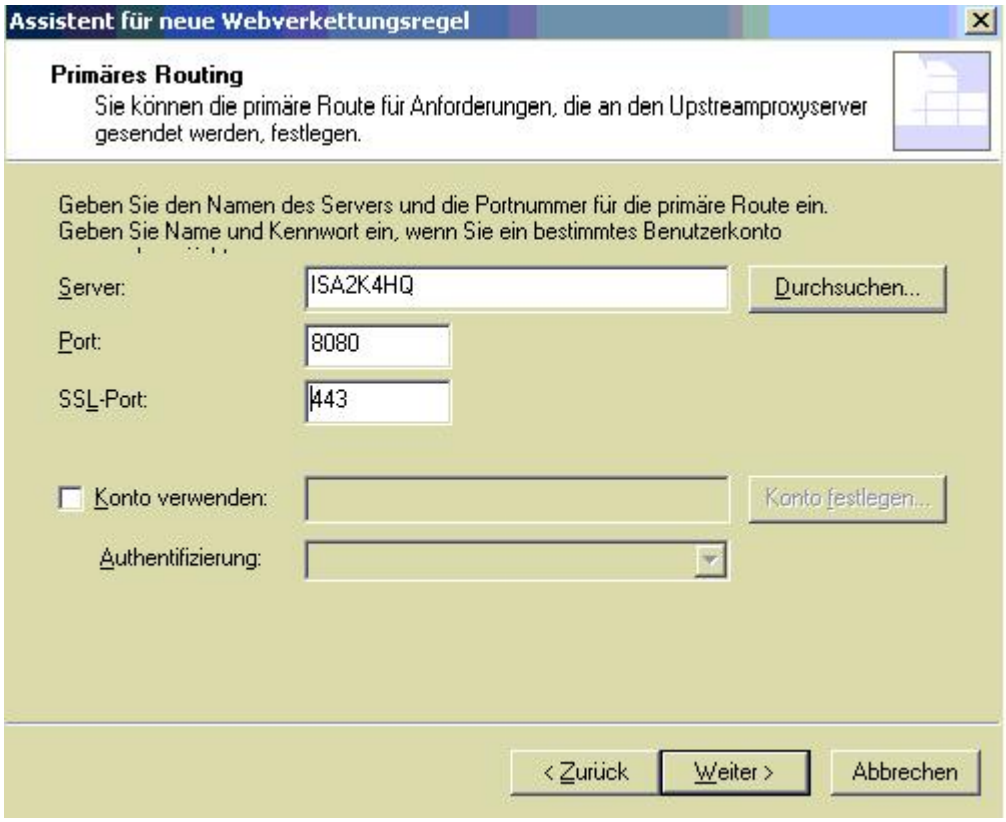
Gibt an, dass ISA Server Anforderungen von Webproxyclients an ein anderes Ziel weiterleitet.
Geben Sie unter Standort die URL des anderen Ziels der Anforderung ein.
Geben Sie unter Port die Portnummer des anderen Ziels ein.
Geben Sie unter SSL-Port die SSL-Portnummer (Secure Sockets Layer) des anderen Ziels ein.

Automatisches Einwählen verwenden

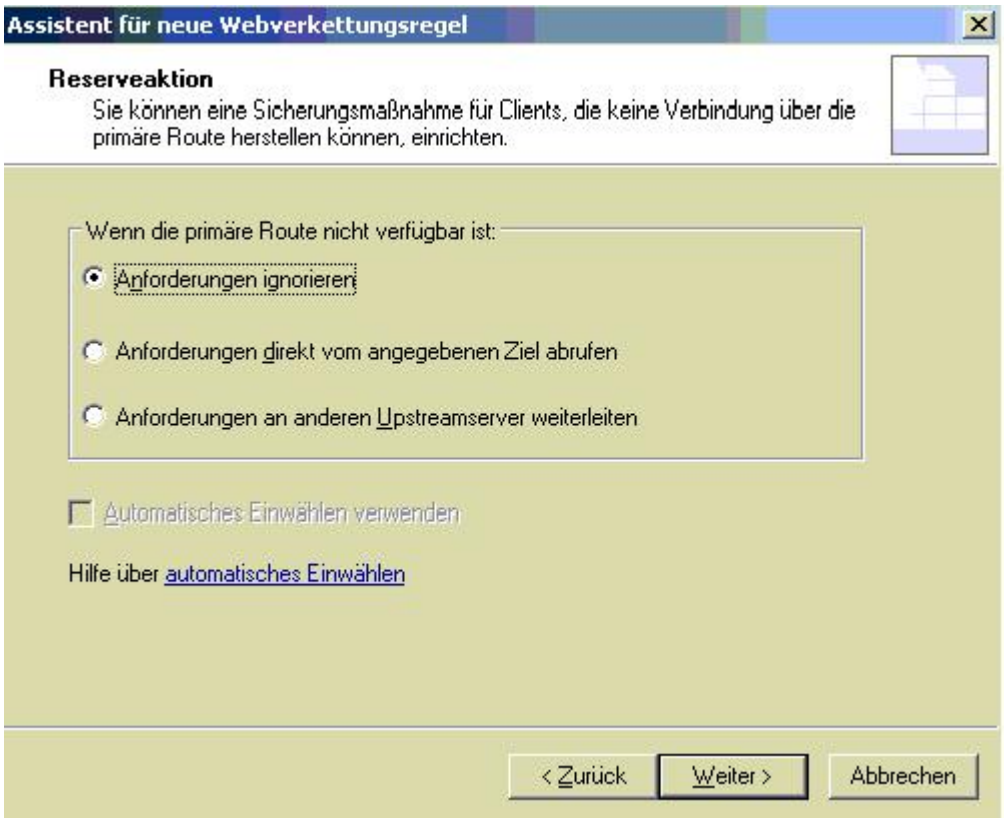
Gibt an, dass ISA Server für die Verbindung zur Primärroute eine DFÜ-Verbindung verwendet. Diese DFÜ Verbindung können Sie ebenfalls in der ISA Verwaltungskonsole erstellen. Ist keine DFÜ-Verbindung vorhanden, bleibt das Feld ausgegraut.



Wenn Sie bei der Anforderungsverarbeitung ***Anforderungen an angegebenen Upstreamserver weiterleiten*** gewählt haben, müssen Sie im Fenster ***Primäres Routing*** den Upstream Proxy und die Port Nummer für HTTP und SSL angeben. Wenn der Upstream Proxy eine Authentifizierung erfordert, müssen Sie auf ***Konto verwenden*** klicken und dort das ***Konto festlegen*** und die Authentifizierungsart (Standard oder WIndows integriert) festlegen.



Im Fenster ***Reserveaktion*** können Sie die Aktion festlegen, wenn die primäre Route nicht verfügbar ist. Aus Redundanzgründen könnten Sie hier einen Reserveserver angeben, indem Sie auf ***Anforderungen an anderen Upstreamserver weiterleiten*** klicken. diesem Beispiel wählen wir ***Anforderungen ignorieren***.



Überprüfen Sie in der Abschlußmeldung des Assistenten noch einmal alle Einstellungen.

Anhand Ihrer Angaben hat der Assistent folgende Webverkettungsregel erstellt.

Zum Schluß können Sie bei Bedarf noch festlegen, wie HTTP- und SSL-Anforderungen weitergeleitet werden sollen. In der Regel ist hier keine Anpassung notwendig.

Klicken Sie zur Anpassung der Weiterleitung mit der rechten Maustaste auf die ***Webverkettungsregel*** und klicken Sie im Kontextmenü auf ***Eigenschaften*** und wählen Sie den Reiter ***Bridging*** aus.

HTTP-Anforderungen umleiten als HTTP-Anforderungen

Legt fest, dass HTTP-Anforderungen als HTTP-Anforderungen umgeleitet werden.

HTTP-Anforderungen umleiten als SSL-Anforderungen

Legt fest, dass HTTP-Anforderungen als SSL-Anforderungen umgeleitet werden. In diesem Fall öffnet ISA Server einen sicheren Kanal zum Server.

SSL-Anforderungen umleiten als HTTP Anforderungen

Legt fest, dass SSL-Anforderungen als HTTP-Anforderungen umgeleitet werden, dass heißt, am ISA Server wird der SSL Tunnel terminiert.

SSL-Anforderungen umleiten als SSL Anforderungen

Legt fest, dass SSL-Anforderungen als SSL-Anforderungen umgeleitet werden. In diesem Fall öffnet ISA Server einen sicheren Kanal zum Server.

Sicherer Kanal (SSL) ist erforderlich

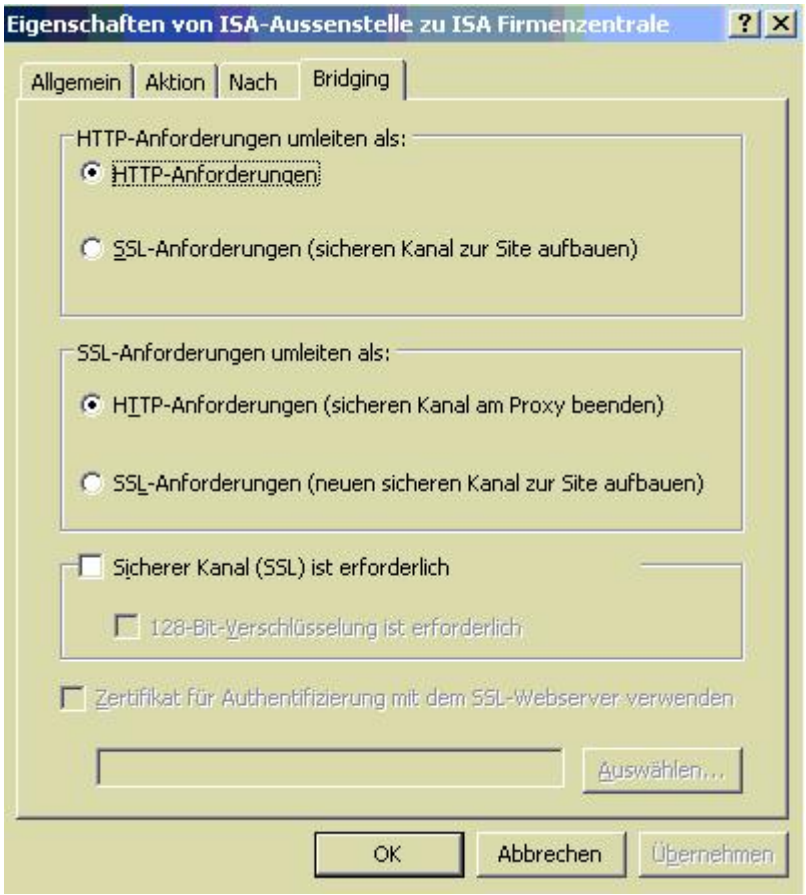
Wählen Sie diese Option aus, um festzulegen, dass der Zugriff nur über einen SSL-Kanal erfolgen darf.

128-Bit-Verschlüsselung ist erforderlich

Klicken Sie auf diese Option, um die 128-Bit-Verschlüsselung auszuwählen.

Zertifikat für Authentifizierung mit SSL-Webserver verwenden

Klicken Sie auf diese Option, um zur Authentifizierung beim SSL-Server ein Zertifikat zu verwenden.
Zertifikate fungieren als zusätzlicher Sicherheitsmechanismus zwischen dem ISA Server 2004 und einem SSL-Webserver.



ISA Server 2004 – Mehrfachnetzwerke - Besonderheiten

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

In meinem ersten Artikel habe ich gezeigt, wie man ein Netzwerk mit ISA Server 2004 definiert. Dieser Artikel beschreibt Besonderheiten der Netzwerkkonfiguration. Schwerpunkt dieses Artikels ist die Beschreibung von typischen Konfigurationsfehlern, Erklärung der Beziehung zwischen ISA Server und Routingtabellen, sowie einiger Tipps aus der Praxis.

Basis für diesen Artikel ist ein ISA Server 2004 Standard mit vier Netzwerkkarten auf einem Windows Server 2003 Standard.

Erklärung der Netzwerke:

- DMZ = Netzwerk für die demilitarisierte Zone
- WAN = Verbindung zum Internet
- LAN = Das interne Netzwerk
- WLAN = Spezielles Netzwerksegment für die WLAN Accesspoint Anbindung.

Wie ein Netzwerk konfiguriert wird, lesen Sie bitte hier. Für weitere Informationen zur Einrichtung einer Firewallrichtlinie finden Sie hier.

Zur Auffrischung: Die Konfiguration eines Netzwerkes erfordert folgende Schritte:

- Erstellen des neuen Netzwerkes und Angabe des Netzwerkbereiches
- Erstellen einer Netzwerkregel welche die verbundenen Netzwerke festlegt und den Typ **ROUTE** oder **NAT** festlegt.
- Erstellen einer Firewallrichtlinie welche den Zugriff zwischen den Netzwerken regelt.

Nach der Installation von ISA Server sind fünf Netzwerke konfiguriert

Intern

Bei dem internen Netzwerk handelt es sich um die IP-Adressbereiche des internen Netzwerkes. ISA Server sieht dieses Netzwerk als vertrauenswürdig (mit Ausnahmen - Stichwort: Systemrichtlinie), aber auch als schutzwürdig an. Die IP-Adressbereiche des Netzwerkobjektes intern müssen mit der Windows Routingtabelle für das interne Interface übereinstimmen.

Externes Standardnetzwerk

Das externe Standardnetzwerk beinhaltet alle IP-Adressen, die nicht ausdrücklich zu einem anderen Netzwerk gehören. Nach der Installation beinhaltet das externe Standardnetzwerk alle Adressen, die nicht im internen Netzwerk enthalten sind, die IP-Adresse des lokalen Hostnetzwerks (127.0.0.1) und die IP-Adressen aller anderen Netzwerkadapter des ISA Server-Computers.

Das externe Standardnetzwerk gilt als **NICHT** vertrauenswürdiges Netzwerk. Daher wird das Netzwerkverhältnis zum externen Standardnetzwerk in der Regel als NAT (Network Address Translation) konfiguriert. Dadurch können Clients des Quellnetzwerks auf externe Standardzielnetzwerke zugreifen, das externe Standardnetzwerk jedoch nicht auf das Quellnetzwerk

Lokaler Host

Dieses Netzwerk steht für den ISA Server-Computer. Das lokale Hostnetzwerk kann **NICHT** geändert oder gelöscht werden.

VPN-Clients

Dieses Netzwerk umfasst die Adressen der derzeit verbundenen Clients. Der Bereich der möglichen Adressen wird bei der Konfiguration der VPN-Eigenschaften festgelegt. Das VPN-Clientnetzwerk kann nicht gelöscht werden.

Quarantänen-VPN-Clients

Zu diesem Netzwerk gehören die Adressen von VPN-Clients, die noch nicht aus der Quarantäne entlassen wurden. Das Quarantänen-VPN-Clientnetzwerk kann nicht gelöscht werden.

Netzwerkvorlagen

ISA Server enthält Netzwerkvorlagen, die häufig vorkommende Netzwerktopologien abbilden. Mithilfe der Netzwerkvorlagen konfigurieren Sie die Firewallrichtlinien für den Datenverkehr zwischen den Netzwerken. Die Verwendung von Netzwerkvorlagen ist nicht zwingend vorgeschrieben. Ein erfahrener Administrator kann die Netzwerke/Netzwerkregeln und Firewallrichtlinien auch per Hand konfigurieren.

ISA Server 2004 enthält die folgenden Netzwerkvorlagen (Auszug aus der Online Hilfe leicht modifiziert):

Edgefirewall

Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle des Netzwerks, dem so genannten Perimeter, befindet. Ein Netzwerkadapter ist hierbei mit dem internen Netzwerk verbunden. Der andere Netzwerkadapter verfügt hingegen über eine Verbindung mit einem externen Netzwerk (Internet). Bei Auswahl dieser Vorlage können Sie den gesamten ausgehenden Datenverkehr zulassen oder den ausgehenden Datenverkehr einschränken, so dass nur der Webzugriff gestattet wird. Eine Edgefirewall gilt nicht als sicherste Firewall Lösung, weil ein Angreifer nur eine Firewall überwinden muß.

3-Abschnitt-Umkreisnetzwerk - (Trihomed Firewall)

Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server mit dem internen Netzwerk, dem externen Netzwerk und einem Umkreisnetzwerk (auch als DMZ, demilitarisierte Zone oder abgeschirmtes Subnetz bezeichnet) verbunden ist. Eine Trihomed Firewall ist eine Firewall mit drei Netzwerkkarten und wird häufig auch als Poor Man's Firewall bezeichnet.

Frontfirewall-Netzwerkvorlage

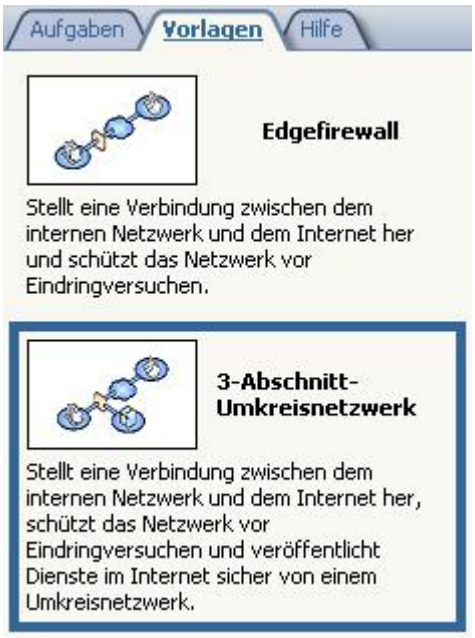
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle eines Netzwerks befindet und zum Schutz des internen Netzwerks ein weiterer Firewall am Back-End konfiguriert ist.

Backfirewall-Netzwerkvorlage

Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server an der Schnittstelle zwischen einem Umkreisnetzwerk und dem internen Netzwerk eingesetzt wird und zum Schutz des internen Netzwerks am Back-End ein weiterer Firewall konfiguriert ist. Weitere Informationen finden Sie unter Backfirewall-Netzwerkvorlage.

Einzelner Netzwerkadapter

Bei dieser Vorlage wird eine Netzwerkkonfiguration mit einem einzelnen Netzwerkadapter angenommen, der sich innerhalb eines Umkreis- oder Firmennetzwerks befindet. In dieser Konfiguration dient ISA Server als Webproxy- und Cacheserver. Diese Netzwerkvorlage entspricht in etwa der Installation eines ISA Server 2000 im Cache Mode.



Hintereinander angeordnete Netzwerke

Sehr häufig stellt sich auch die Frage, wie der ISA Server konfiguriert werden muss, wenn sich die Netzwerke hintereinander angeordnet befinden, dass heißt, sich hinter dem ISA Server weitere Netzwerke als das interne Netzwerk befinden.

Bei einer Konfiguration hintereinander angeordneter Netzwerke verfügt ein Netzwerkadapter über Routen zu einem fremden Netzwerk. In den meisten Fällen unterstützt ISA Server derartige Konfigurationen nicht, wobei jedoch folgende Ausnahmen gelten:

- Ein IPSec-Tunnel der zwischen zwei Standorten besteht.
- Das vordefinierte externe Netzwerk kann sich hinter dem als Standardgateway dienenden Netzwerkadapter befinden.
- Quarantänen-VPN-Clients können niemals direkt mit einem Netzwerk verbunden sein.

Angenommen, ein Netzwerkadapter mit der Adresse 10.0.0.1 ist das Standardgateway. Außerdem verfügt dieser Netzwerkadapter über Routen zu den Adressen ...
10.X.X.X und
30.X.X.X,
wobei keine Routen (in keinem Netzwerkadapter) für die Adressen 20.X.X.X vorhanden sind. Weiterhin wird in diesem Szenario davon ausgegangen, dass Sie zwei Netzwerke eingerichtet haben:
Netzwerk A: 10.0.0.0–10.255.255.255
Netzwerk B: 30.0.0.0–30.255.255.255
Es sind keine Routen für die Netzwerkadressen im Bereich 20.0.0.0–20.255.255.255 definiert, daher werden diese als Teil des externen Standardnetzwerks angesehen.

Das externe Standardnetzwerk wird als "hinter Netzwerk A befindlich" angesehen, da der Adapter von Netzwerk A eine Route zum externen Standardnetzwerk besitzt, jedoch diesem Netzwerk nicht zugeordnet ist. (Die Adresse des Adapters gehört nicht zum externen Netzwerk.)
Netzwerk B befindet sich dieser Definition nach ebenfalls hinter Netzwerk A. Allerdings ist Netzwerk B nicht das externe Standardnetzwerk. ISA Server betrachtet dies jedoch als eine fehlerhafte Konfiguration und das Netzwerk wird vorübergehend getrennt.

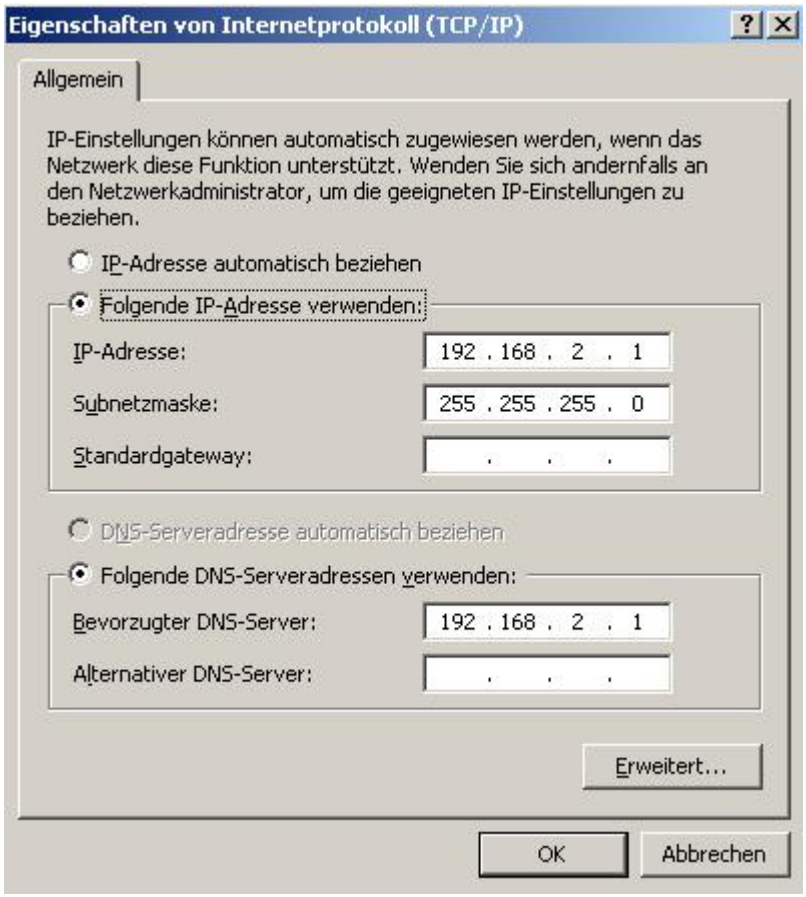
Zur Konfiguration von ISA Server werden die beiden Routen (zu 10.X.X.X und 30.X.X.X) in einem einzelnen Netzwerk zusammengefasst. ISA Server kann diese beiden Adressbereiche nicht als eindeutige Netzwerke auffassen, da beide demselben Netzwerkadapter zugeordnet sind.

ISA Server Fehlermeldung "ISA Server hat Routen über den Adapter "XXXXX" ermittelt, die mit dem Netzwerkelement, dem dieser Adapter angehört, nicht übereinstimmen."

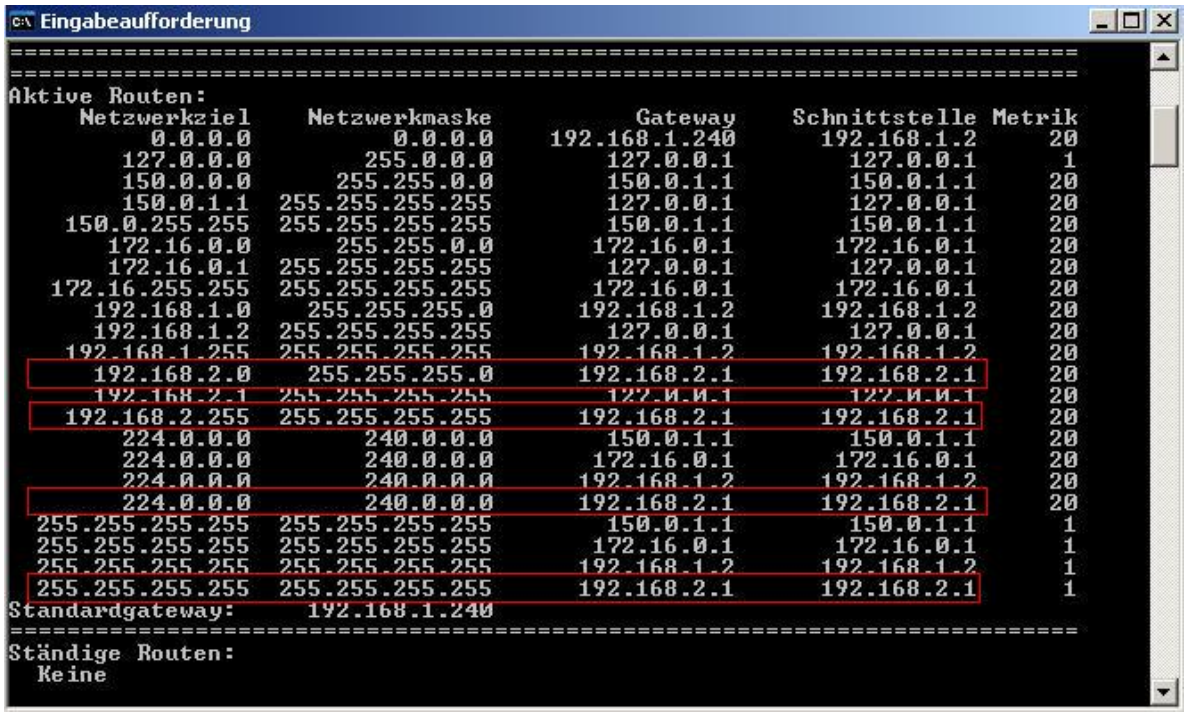
Auf diese Fehlermeldung suchen viele Administratoren seit Erscheinen des ISA Server 2004 in den Newsgroups eine Antwort zur Lösung des Problems. Aus diesem Anlass sollen hierzu einige klärende Worte gesagt werden.

Das (korrekt konfigurierte) interne Netzwerk in diesem Artikel ist wie folgt definiert:

Das interne Netzwerkinterface am ISA hat folgende Konfiguration:



ISA Server versucht bei der Ermittlung des Netzwerkobjektes einen Netzwerkadapter zu finden, der eine IP-Adresse aus diesem Netzwerkbereich hat.
ISA Server ermittelt diese Informationen anhand der Windows 2003 Routingtabelle.
Achten Sie in diesem Beispiel auf die Schnittstelle **192.168.2.1.** Es folgt ein Auszug der Windows 2003 Routingtabelle.



Von Bedeutung für den ISA Server ist hier nur die Route ...

192.168.2.0 255.255.255.0 192.168.2.1 192.168.2.1

Bei den anderen Routen handelt es sich um Multicast / Broadcast Adressen und müssen nicht berücksichtigt werden.

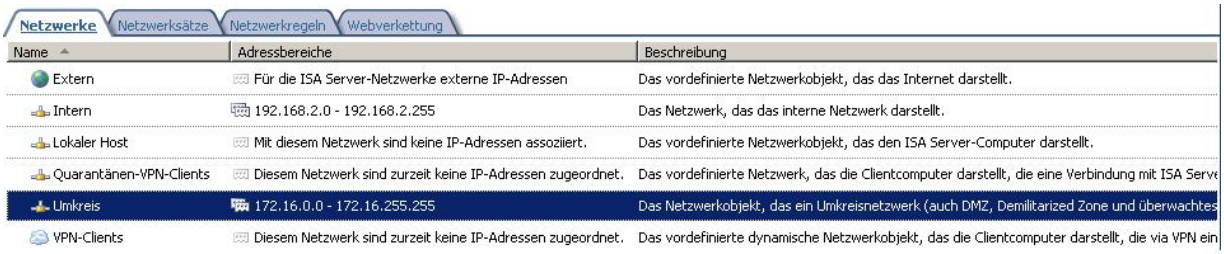
Erläuterung der anderen Routen:
0.0.0.0 ist die Default Route
127.0.0 ist die Loopback-Adresse
192.168.2.0 ist die Netzwerk-Route für das Netzwerk 150.3.0
192.168.2.1 (255.255.255.255) ist die Host-Route des lokalen Hosts
192.168.2.255 ist die Subnetz-Broadcast-Adresse
224.0.0.0 ist für das Multicasting
255.255.255.255 ist für die limitierte Broadcast-Adresse

Die oben beschriebene Fehlermeldung tritt dann auf, wenn Routen nicht mit dem internen Netzwerkobjekt übereinstimmen oder der IP-Adressbereich des internen Netzwerkobjektes nicht richtig definiert wurde. Ein falsch konfiguriertes Netzwerk kann dazu führen, dass ISA Server das Netzwerk nicht schützen kann weil Adressbereiche falsch interpretiert werden.

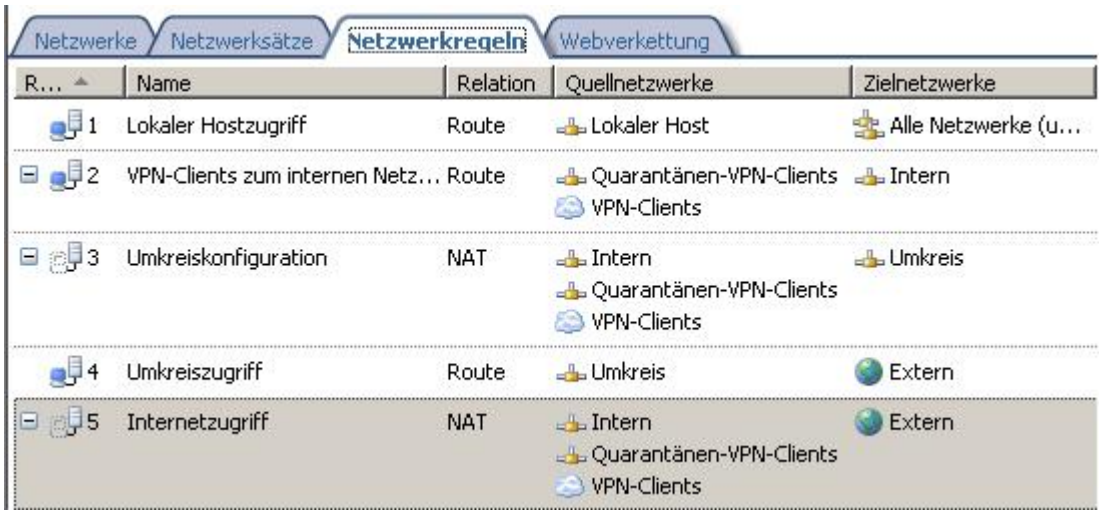
Eine detaillierte Erklärung zu diesem Thema finden Sie hier.

Trihomed DMZ Beispiel

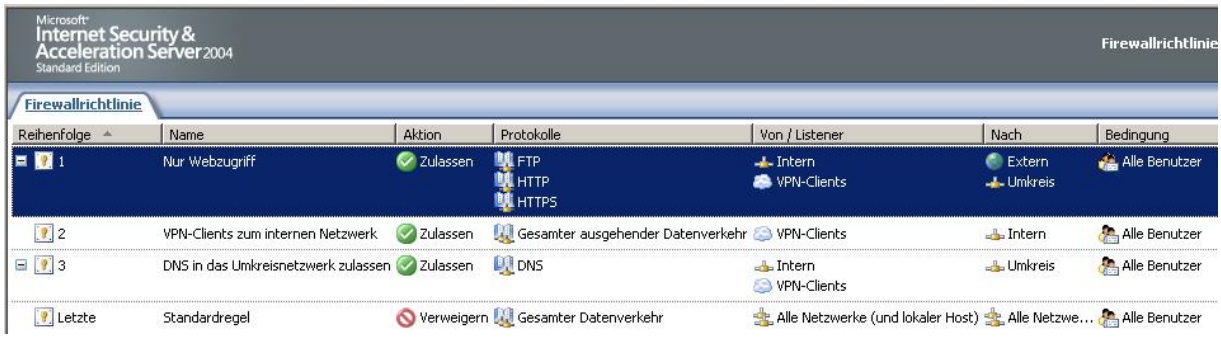
Zum Abschluss dieses Artikels ein Beispiel einer ISA Server 2004 Konfiguration mit der Netzwerkvorlage 3-Abschnitt Umkreisnetzwerk.
Die folgenden Grafiken sollen Ihnen einen Überblick über die Flexibilität des ISA Servers in Bezug auf die Multinetwork-Funktionalitäten geben.
Sie sehen hier ein Netzwerk mit dem Namen Umkreis, welches das Umkreisnetzwerk, auch DMZ genannt, darstellt.



Die Netzwerkregel ist auf **NAT** für interne Kommunikation mit dem Umkreisnetzwerk und **ROUTE** vom Umkreisnetzwerk mit **EXTERN** konfiguriert.



Für das neu erstellte Netzwerk wird basierend auf der gewählten Einstellung des Wizard eine entsprechende Firewallrichtlinie erstellt.



ISA Server 2004 – IP-Einstellungen definieren

Die Informationen in diesem Artikel beziehen sich auf:

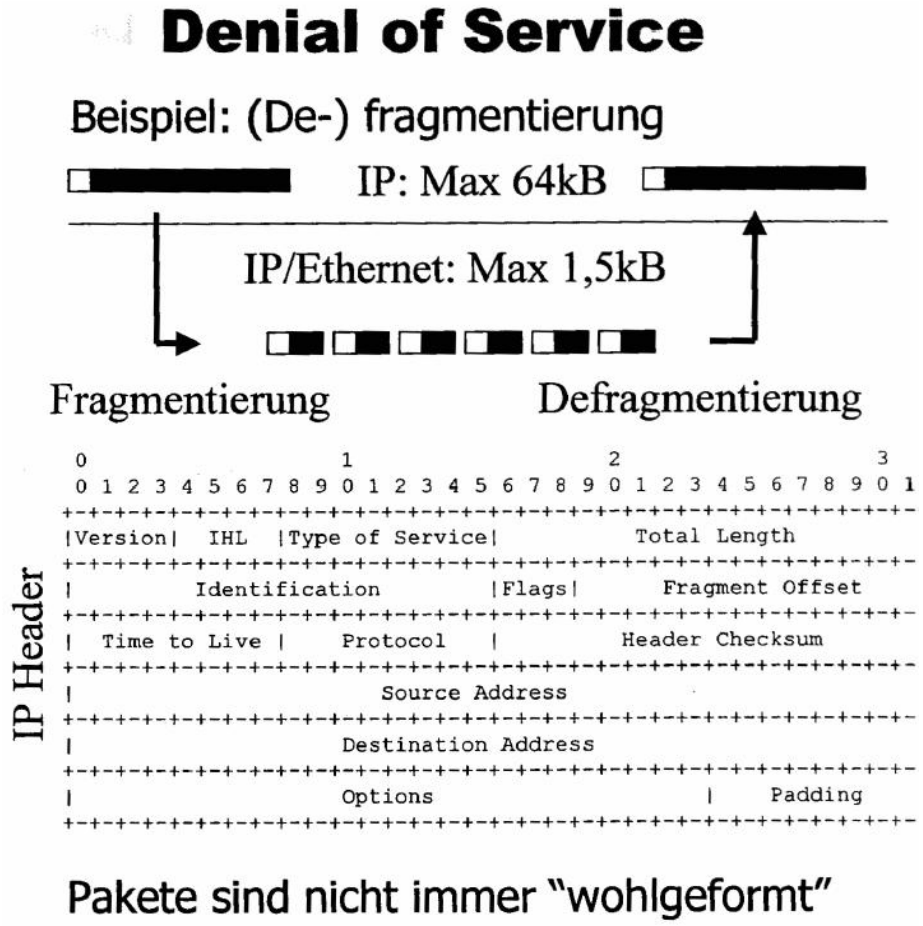
- Microsoft ISA Server 2004

Einleitung

ISA Server 2004 bietet die Option zur Konfiguration von IP-Einstellungen, um die Sicherheit des Systems zu erhöhen. Befolgen Sie bei der Konfiguration den Hinweisen in diesem Artikel:

IP-Optionen

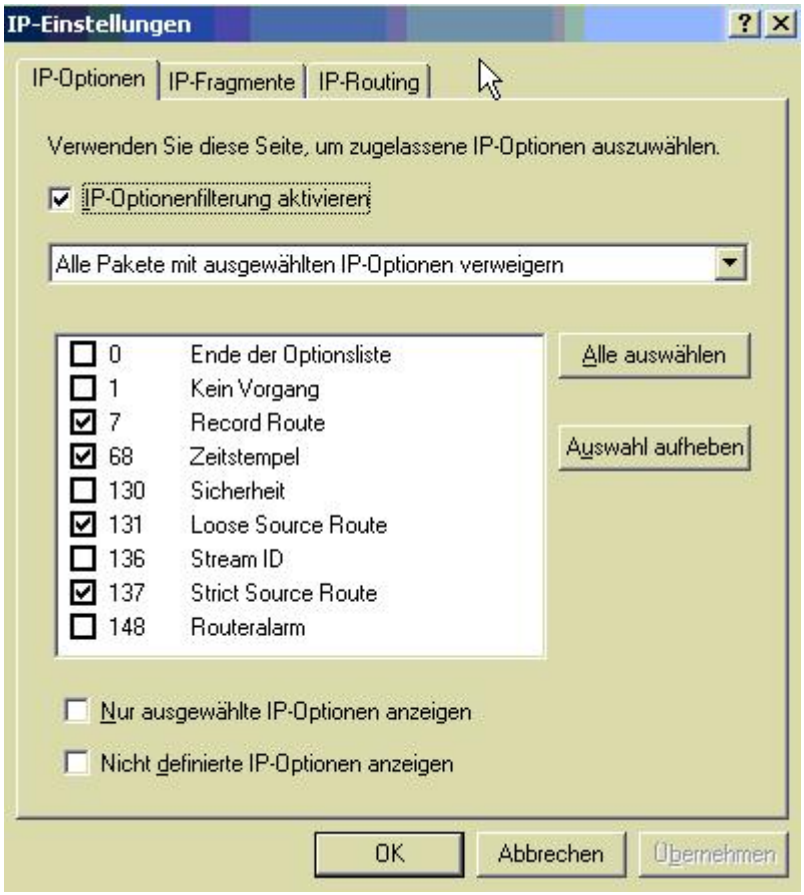
Bei den IP-Optionen handelt es sich um einen speziellen Bereich im IP-Header mit dem Namen IP-Options.
IP-Optionen definieren zusätzliche Möglichkeiten des IP Protokolls wie z. B. die bekannteste IP-Option 9 - Strict Source Route. Es gibt die Möglichkeit 256 IP-Optionen zu konfigurieren (0-255).

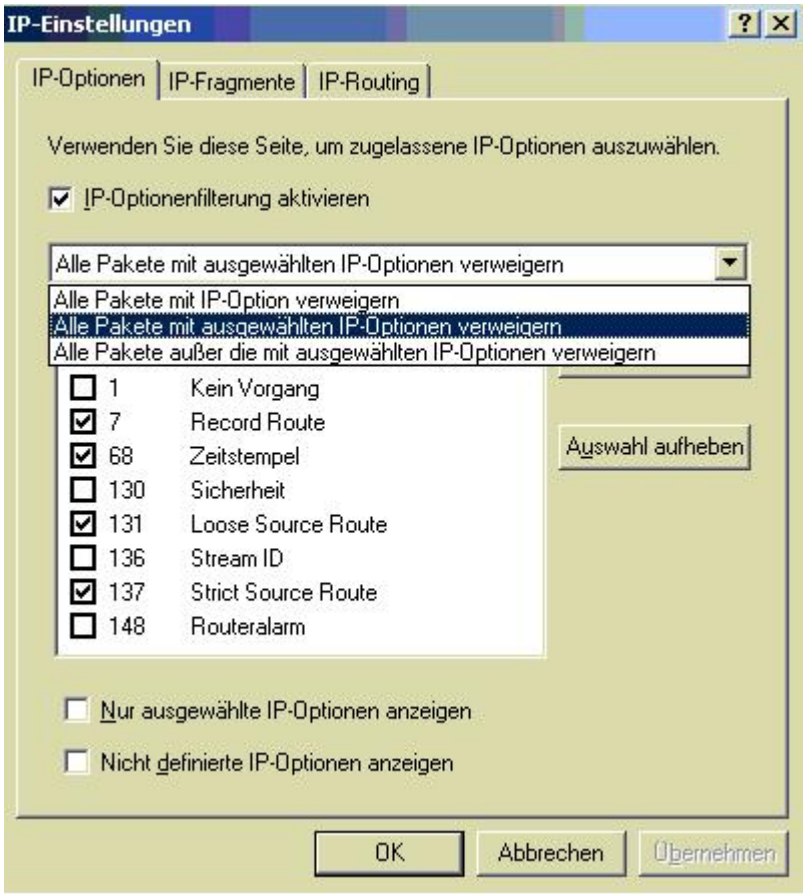


ISA Server 2004 blockiert einige IP-Optionen weil diese für Angriffe genutzt werden können. Nehmen wir als Beispiel nochmal die IP-Option 9: Die einfachste Routing – Attacke benutzt die Internet – Protokolloption 9 bzw. 3 In beiden Fällen kann die Route durch das Netzwerk vom Sender des IP-Paketes bestimmt werden. Bei Verwendung von "Strict Source Routing" muss dabei jeder Vermittlungsknoten in der richtigen Reihenfolge angegeben werden. Im Gegensatz zu "Loose Source Routing" welches auch zusätzliche Hops zwischen zwei angegebenen IP – Adressknoten zulässt. Der Datenstrom der Zielstation kann damit problemlos an das Computersystem des Eindringlings "umgeleitet" werden. Dazu simuliert der Angreifer wiederum die IP – Adresse eines internen Systems (IP – Adress – Spoofing) und öffnet unter Aktivierung der Option "Loose Source Routing" eine Verbindung zur Zielstation, wobei als Route für die Antwortpakete ein Pfad, der über das angreifende System führt, angegeben wird. Damit stehen dem eingedrungenem System alle Möglichkeiten der simulierten, internen Station zur Verfügung.

Im ISA Server 2004 wird Strict Source Route als IP Option 137 und Loose Source Route als IP Option 131 dargestellt.

Für die Standardinstallationen können Sie die IP-Optionen aktiviert lassen und müssen keine zusätzlichen IP-Optionen aktivieren. Aktivieren Sie zusätzliche IP-Optionen nur, wenn Sie deren Bedeutung vollständig verstehen.

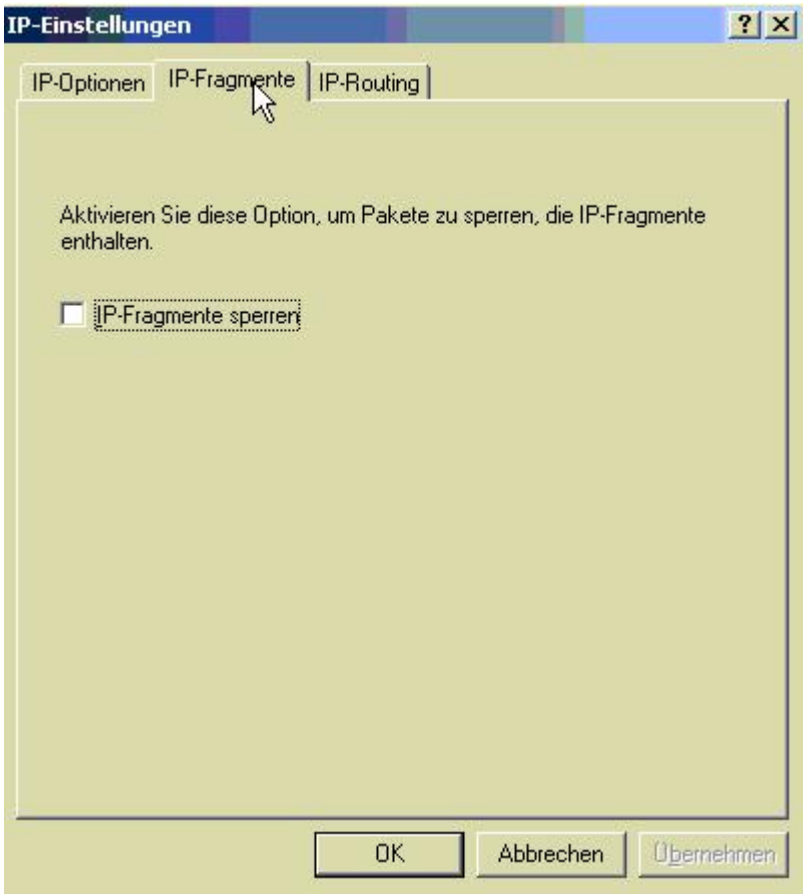

IP-Einstellungen
IP-Optionen
IP-Fragmente
IP-Routing
Verwenden Sie diese Seite, um zugelassene IP-Optionen auszuwählen.
IP-Optionenfilterung aktivieren
Alle Pakete mit ausgewählten IP-Optionen verweigern
0 Ende der Optionsliste
1 Kein Vorgang
7 Record Route
68 Zeitstempel
130 Sicherheit
131 Loose Source Route
136 Stream ID
137 Strict Source Route
148 Routeralarm
Alle auswählen
Auswahl aufheben
Nur ausgewählte IP-Optionen anzeigen
Nicht definierte IP-Optionen anzeigen
OK
Abbrechen
Übernehmen


IP-Einstellungen
IP-Optionen
IP-Fragmente
IP-Routing
Verwenden Sie diese Seite, um zugelassene IP-Optionen auszuwählen.
IP-Optionenfilterung aktivieren
Alle Pakete mit ausgewählten IP-Optionen verweigern
Alle Pakete mit IP-Option verweigern
Alle Pakete mit ausgewählten IP-Optionen verweigern
Alle Pakete außer die mit ausgewählten IP-Optionen verweigern
1 Kein Vorgang
7 Record Route
68 Zeitstempel
130 Sicherheit
131 Loose Source Route
136 Stream ID
137 Strict Source Route
148 Routeralarm
Auswahl aufheben
Nur ausgewählte IP-Optionen anzeigen
Nicht definierte IP-Optionen anzeigen
OK
Abbrechen
Übernehmen

IP-Fragmente

In den unterschiedlichsten Netzwerken ist die Länge der übertragenen IP-Pakete immer eingeschränkt und Toplogieabhängig. Abhängig von dem verwendeten Netz wird die maximale Größe der IP-Pakete in als Maximum Transfer Unit (MTU) in Oktetten (Bytes) angegeben. Zur Anpassung der übertragenen IP-Pakete an unterschiedliche MTU-Werte ist das IP-Protokoll in der Lage, Pakete entsprechend den MTU-Werten der einzelnen Netze zu fragmentieren, dass heisst, große IP-Pakete auf eine Reihe von kleineren IP-Teilpaketen (IP-Fragmenten) aufzuteilen. Ein Quellrechner kann auch verbieten, dass ein IP-Paket fragmentiert werden darf. Hierfür muss der Quellrechner/Router das Bit DF (don´t fragment) im Feld Flags des IP-Headers auf 1 setzen. Die Größe des IP-Pakets liegt bei 576 bis 65 536 Oktetten. Wenn man die minimale Länge von 20 Oktetten des IP-Headers berücksichtigt, bleiben für die weiteren Daten und den TCP-Header noch 65 516 Oktette. Die minimale Größe von 576 Oktetts muss von jeder IP-Implementierung unterstützt werden.

ISA Server 2004 deaktiviert das Blocken von IP-Fragementen per Default, weil ein aktviertes blocken von IP-Fragmenten auch zu unerwünschten Nebeneffekten führen kann, dass zum Beispiel VPN und IPSEC Verbindungen Probleme bereiten, da ja hier bewusst IP Pakete vor Veränderung geschützt werden. IP-Fragmente können aber auch die Sicherheit des Systems gefährden. Ein Beispiel für einen Sabotageangriff ist der Ping-of-Death, bei dem ein synthetisches, unzulässig großes IP-Paket (>65535 Bytes) in fragmentierter Form übertragen wird. Das angegriffene System stürzt bei dem Versuch ab, die Fragmente wieder zusammenzufügen. Das ist sicherlich kein aktuelles Beispiel, weil alle aktuellen Firewallsysteme in der heutigen Zeit gegen Ping of Death gefeit sind, (auch der ISA Server hat einen IDS gegen Ping of Death (lizenziert von ISS)) soll aber als Beispiel ausreichend sein.



IP-Routing

Wenn IP-Routing aktiviert ist, sendet ISA Server das ursprüngliche Netzwerkpaket zum Ziel. Durch IP-Routing wird zwar der Durchsatz verbessert, aus Sicherheitsgründen wird jedoch empfohlen, diese Funktion zu deaktivieren. Wenn IP-Routing deaktiviert ist, sendet ISA Server nur die Daten (nicht das gesamte Paket) zum Ziel. ISA Server 2004 verwaltet sekundäre NAT Verbindungen von komplexen Protokollen (z. B. FTP) direkt im Kernel Mode, welches den Durchsatz für Protokolle mit sekundären Protokollen erheblich beschleunigen kann. Sekundäre Verbindungen für Secure NAT Clients werden allerdings nur unterstützt wenn ein Applikations-Filter für das Protokoll auf dem ISA Server 2004 installiert ist. Sie müssen also hier eine Entscheidung zu Gunsten der Performance (aktiviertes IP-Routing) oder zu Gunsten der Sicherheit (deaktiviertes IP-Routing) treffen. Aufgrund der Tatsache, dass IP Routing per Default aktiv ist und auch andere Firewallimplementationen per Default IP Routing aktivieren, können Sie diese Einstellung unverändert lassen.

Konfiguration des ISA für automatische Suche der Clienteinstellungen (WPAD/WSPAD)

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Die automatische Suchfunktion des ISA Server ermöglicht die Konfiguration von Clients, sodass sie automatisch den entsprechenden ISA Server-Computer suchen und finden. Auf diese Weise können zum Beispiel mobile Clients eine Verbindung zum nächstgelegenen ISA Server-Computer herstellen. Dies ist besonders für Unternehmen mit mehreren Standorten interessant. Jeder Standort ist durch einen eigenen ISA Server geschützt, hat aber ein anderes IP-Netzwerk. Benutzer, die mit ihren Notebook zwischen den einzelnen Standorten wechseln, müssen keine Konfigurationsänderungen am Webbrowser und/oder Firewallclient vornehmen. Durch Aktivieren der automatischen Suche suchen alle Webproxy- und Firewallclients automatisch den entsprechenden ISA Server-Computer. Dies senkt auch den administrativen Aufwand erheblich, denn künftig müssen bei Netzwerkveränderungen die Clients nicht mehr manuell angepasst werden.

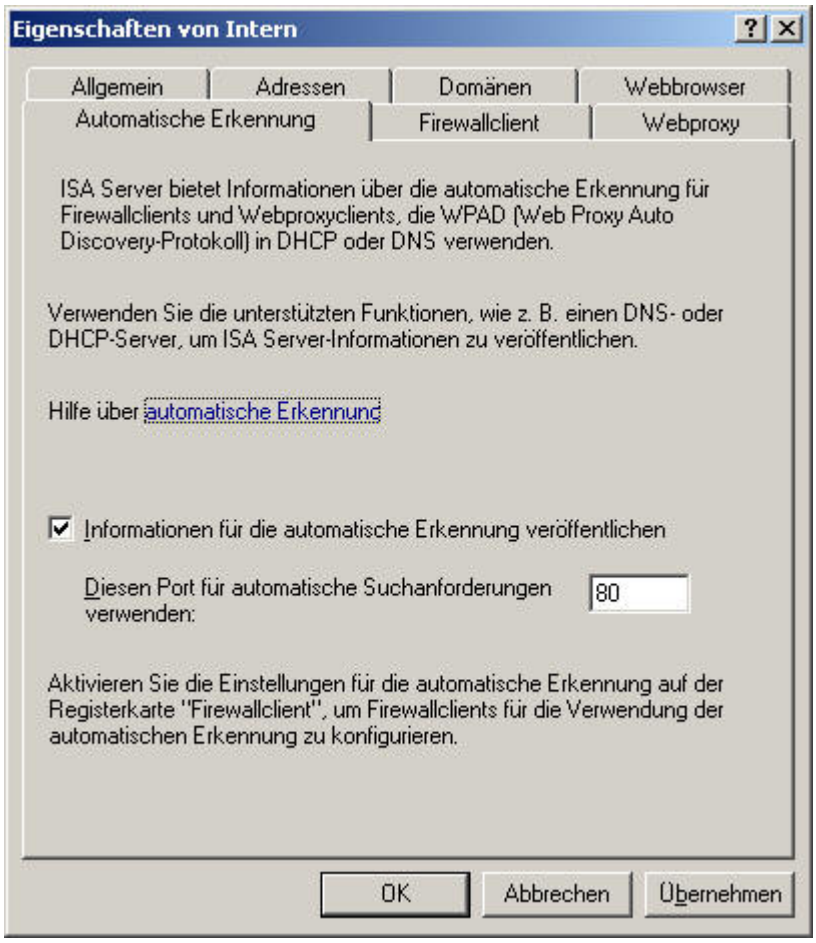
Voraussetzung für das Webproxy Autodiscovery Protokoll (WPAD) bzw. Winsock Proxy Autodiscovery Protokoll (WSPAD) ist eine funktionierende DNS- und/oder DHCP-Umgebung. Wenn die automatische Suche konfiguriert ist, verbinden sich die Webproxy- oder Firewallclients mit dem DNS oder DHCP-Server und fragen nach einem WPAD-Eintrag, der auf den ISA Server verweist. Wenn der WPAD-Eintrag zur Verfügung gestellt werden kann können die Clients den angegebenen ISA Server verwenden. WPAD setzt einen Internet Explorer 5.0 oder höher voraus. WPAD/WSPAD über DNS wird von Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows 98 und Windows Me unterstützt. WPAD/WSPAD über DHCP ist für Windows Server 2003, Windows XP, Windows 2000, Windows 98 und Windows Me nutzbar.

Neben den angesprochenen Einstellungen am DNS- oder DHCP-Server ist eine (einfache) Einstellung am ISA Server vorzunehmen. Alle Konfigurationsdetails werden nachfolgend erläutert:

1. Einstellungen am ISA Server zur Veröffentlichung der WPAD-Informationen

WPAD-Informationen können für jedes interne Netzwerk individuell festgelegt werden.

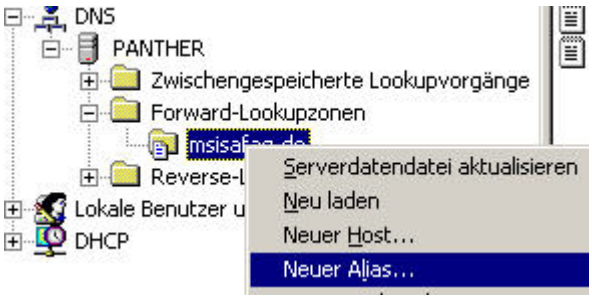
In den Eigenschaften des internen Netzwerkes (ISA Verwaltungskonsole -> [Servername] -> Konfiguration -> Netzwerke -> [Netzwerkname]) gibt es die Registerkarte "Automatische Erkennung":

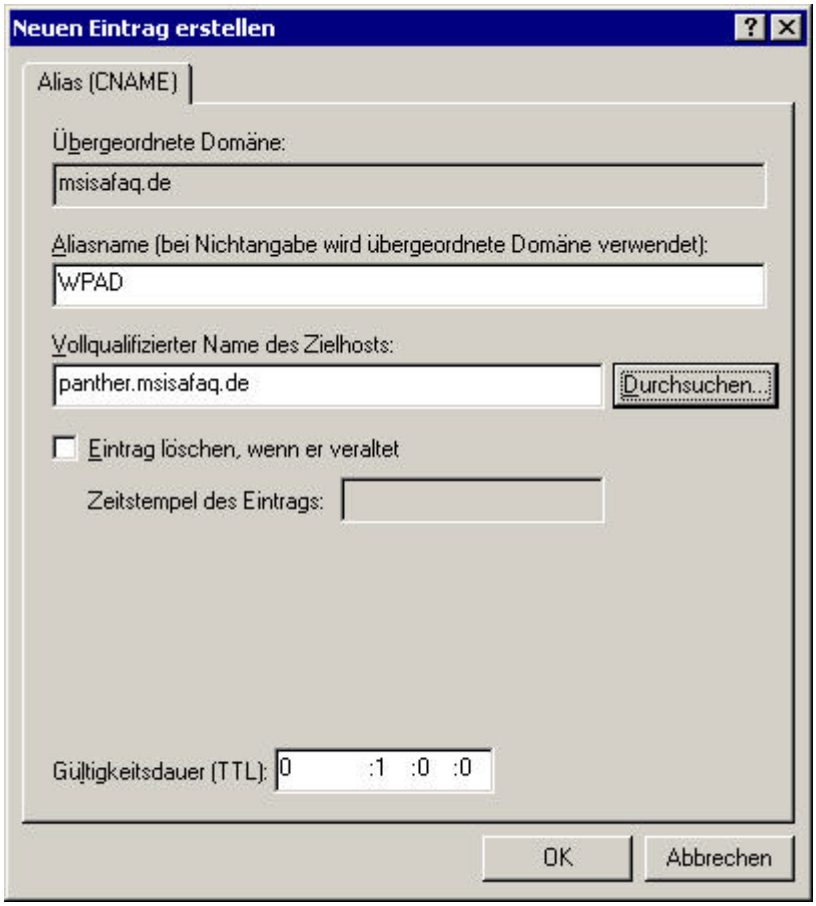


Der Port kann auch geändert werden, wenn er z.B. durch den IIS belegt ist. Der Port 80 beißt sich hier nicht mit dem Port für ausgehende Webanfragen.

2. Konfiguration der DNS-Einstellungen

In der internen DNS-Zone muss ein CName-Record (Alias) für den ISA Server eingerichtet werden:

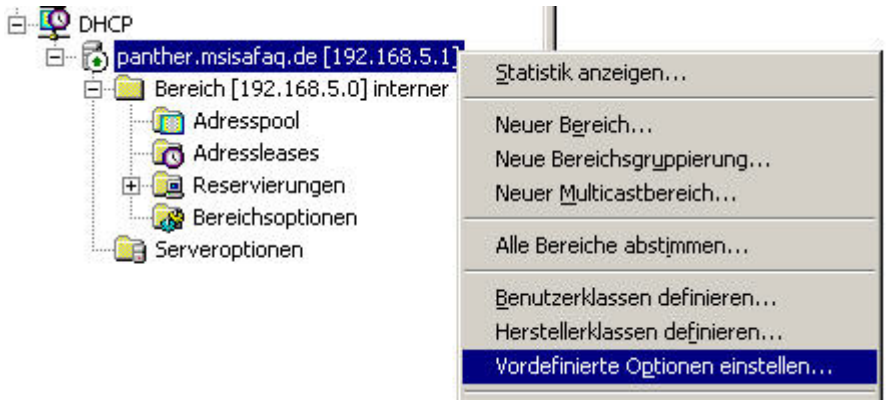


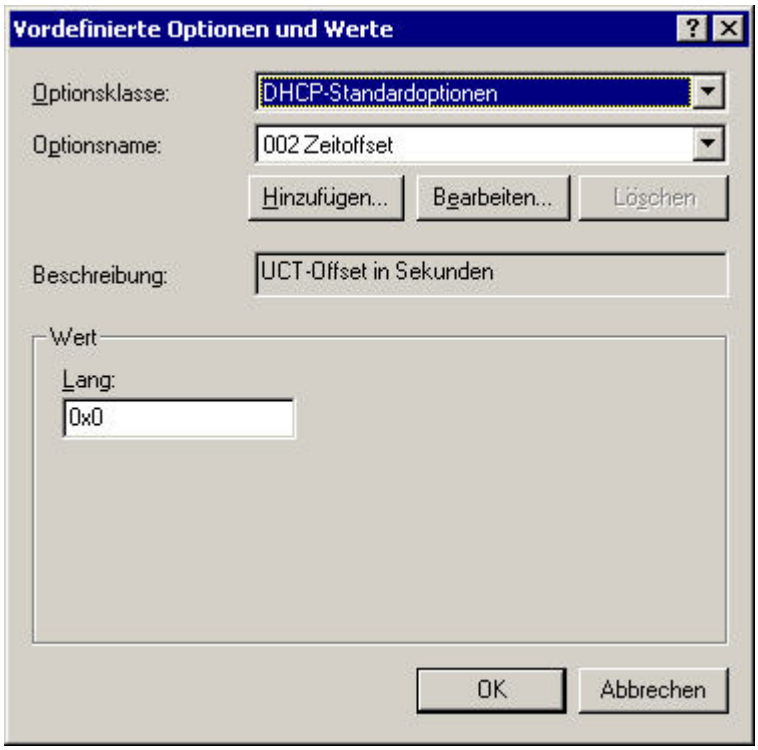


Der Aliasname muss WPAD lauten, im nächsten Eingabefeld wird der komplette Domänenname des ISA Servers eingetragen. In diesem Beispiel heißt der Server "Panther", die Domäne lautet msisafaq.de.

3. Konfiguration der DHCP-Einstellungen

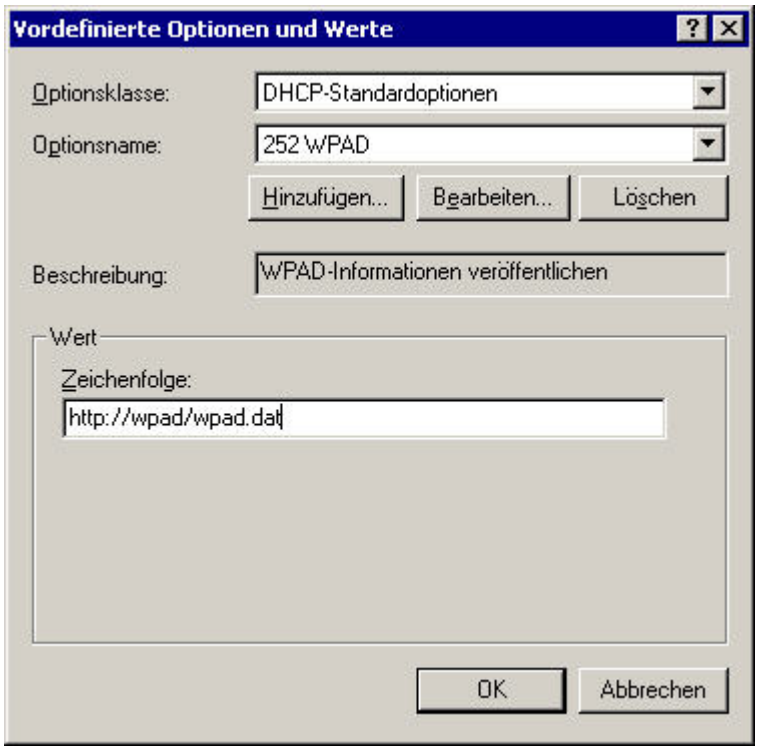
Es muss eine neue vordefinierte Option im DHCP-Server erstellt werden:





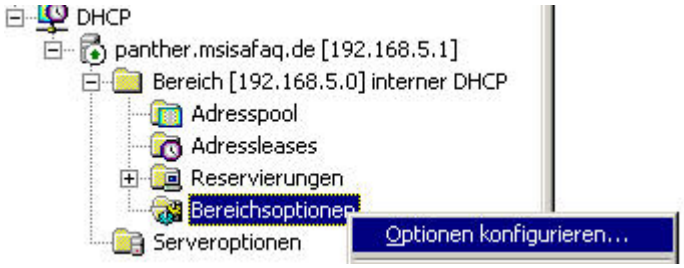
Es muss ein neuer Optionsname "WPAD" mit folgenden Daten eingerichtet werden:

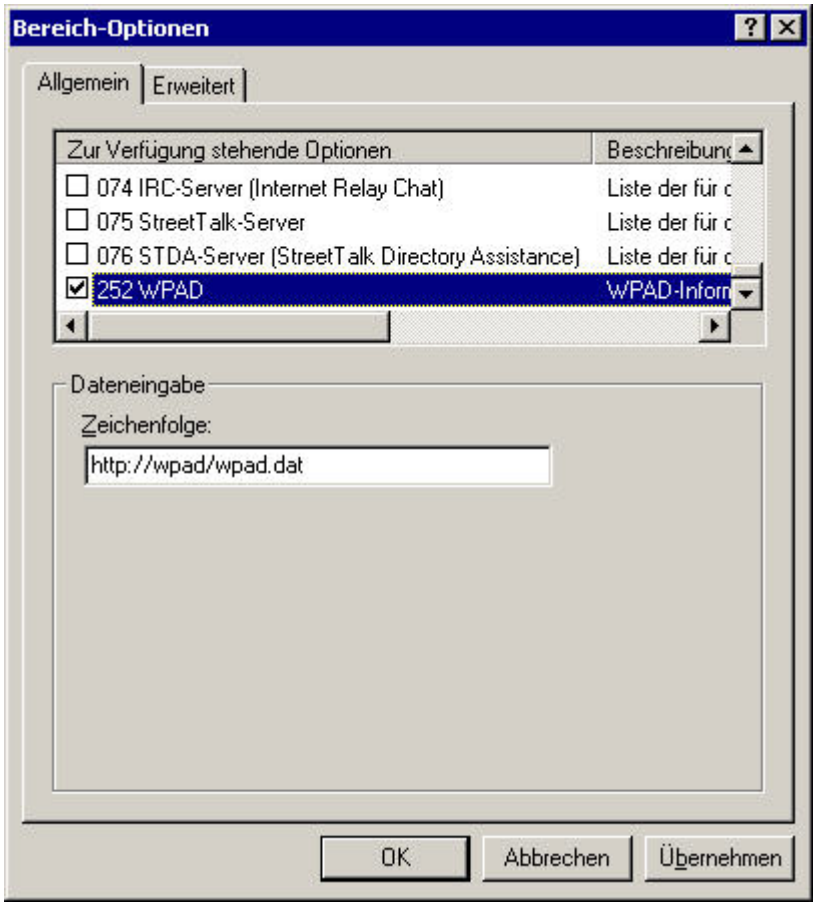
Nachdem der Optionsname erstellt wurde, wird er auch verwendet.



Als Zeichenfolge wird der Pfad zum ISA Server eingetragen. Wurde ein entsprechender DNS-Eintrag erstellt und der Port im ISA auf 80 belassen, reicht obiger Eintrag aus. Der Einzutragende Name hat grundsätzlich das Format http://Computername:AutoDiscoveryPortNummer/Wpad.dat wobei *Computername* den vollqualifizierten Domänennamen des ISA Server-Computers und *AutoDiscoveryPortNummer* die Portnummer darstellt, auf der die Informationen für die automatische Suche veröffentlich werden. Dieser Port stimmt entweder mit der Portnummer für ausgehende Webanfragen oder einem zusätzlichen Port überein, der für die Veröffentlichung der automatischen Suche verwendet wird.

Als nächstes muss die soeben erstellte Option auch verwendet werden. Je nach DHCP-Konfiguration kann das in den Server- oder in den Bereichsoptionen eingestellt werden.





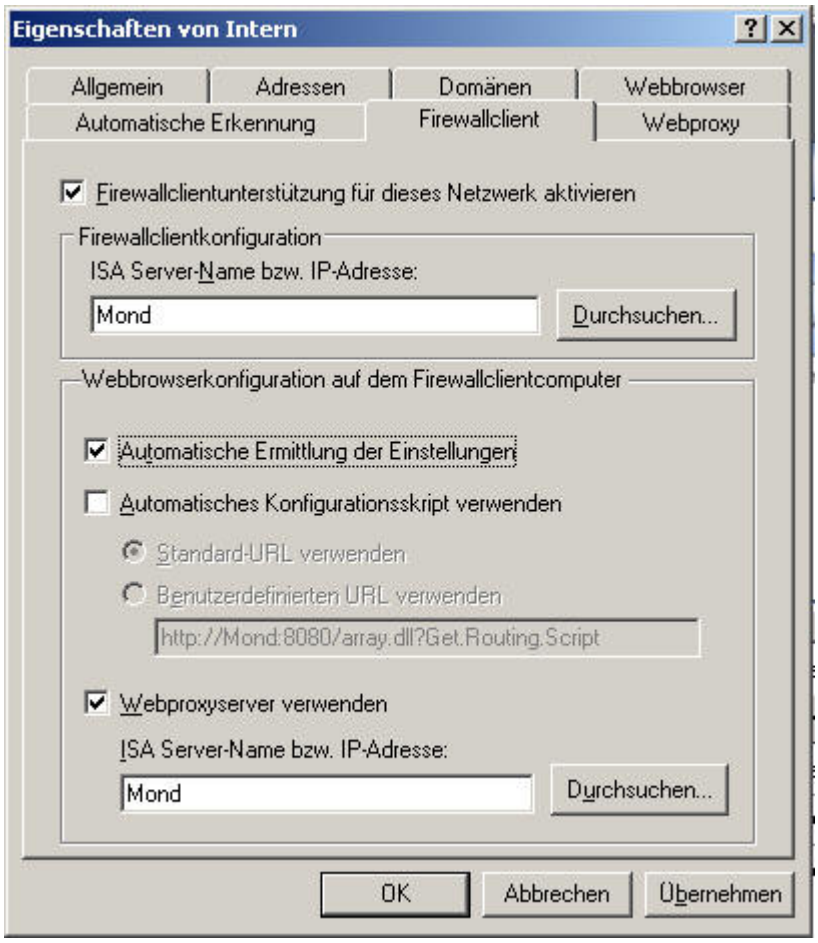
Es muss sichergestellt werden, dass die Option 252 aktiviert ist. Ein Beispiel für einen konfigurierten DHCP-Bereich mit Optionen könnte so aussehen:

Optionsname	Hersteller	Wert	Klasse
003 Router	Standard	192.168.5.1	Keine
006 DNS-Server	Standard	192.168.5.1	Keine
015 DNS-Domänenname	Standard	msisafaq.de	Keine
252 WPAD	Standard	http://wpad/wpad.dat	Keine

4. Konfiguration der Clienteinstellungen für Firewallclients

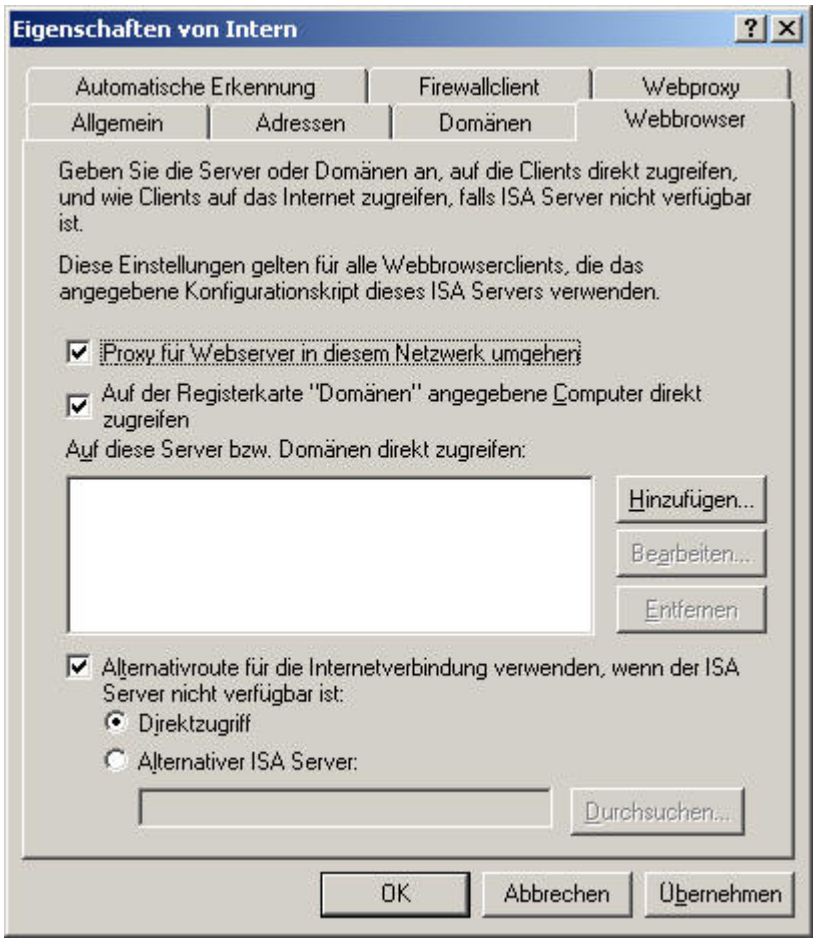
Um die Einstellungen für die automatische Suche den Clients bei der Installation des Firewallclients mitzugeben, kann dies am ISA Server eingestellt werden.

Dazu werden weder die Eigenschaften internen Netzwerks geöffnet:



Durch diese Einstellung wird der Internet Explorer auf Clientcomputern, die den Firewallclient installiert haben, automatisch für WPAD konfiguriert und somit zum Webproxyclient.

In den Eigenschaften des Netzwerkes können auf der Registerkarte "Webbrowser" noch weitere Optionen konfiguriert werden:

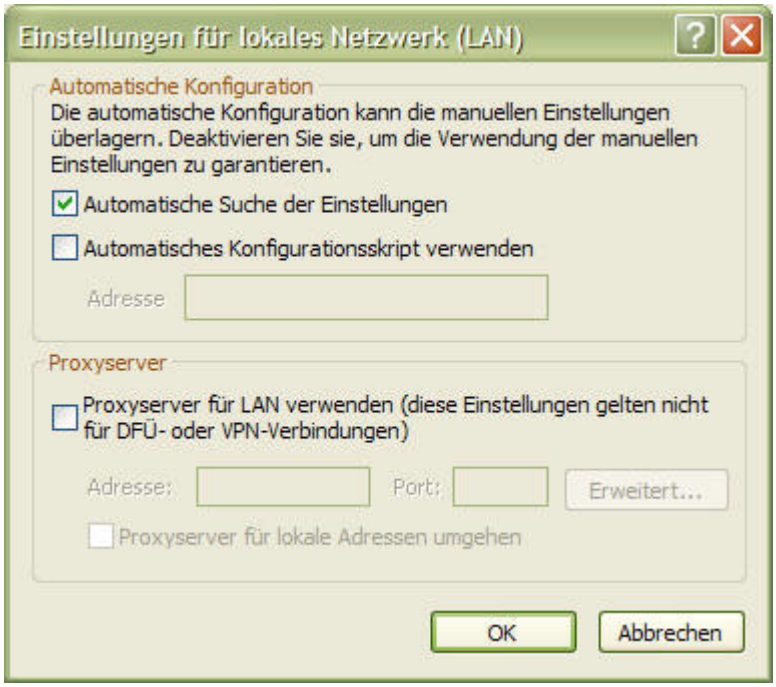


Sofern z.B. im internen Netzwerk Webserver stehen, sollten diese direkt und ohne Proxyserver angesprochen werden. Dazukönnen diese Server oder Serverbereiche im obigen Feld als Proxyausnahmen eingetragen werden.

5. Konfiguration des Webbrowsers für die Automatische Suche

Wenn kein Firewallclient installiert ist, muss der Internet Explorer ggfs. manuell angepasst werden:

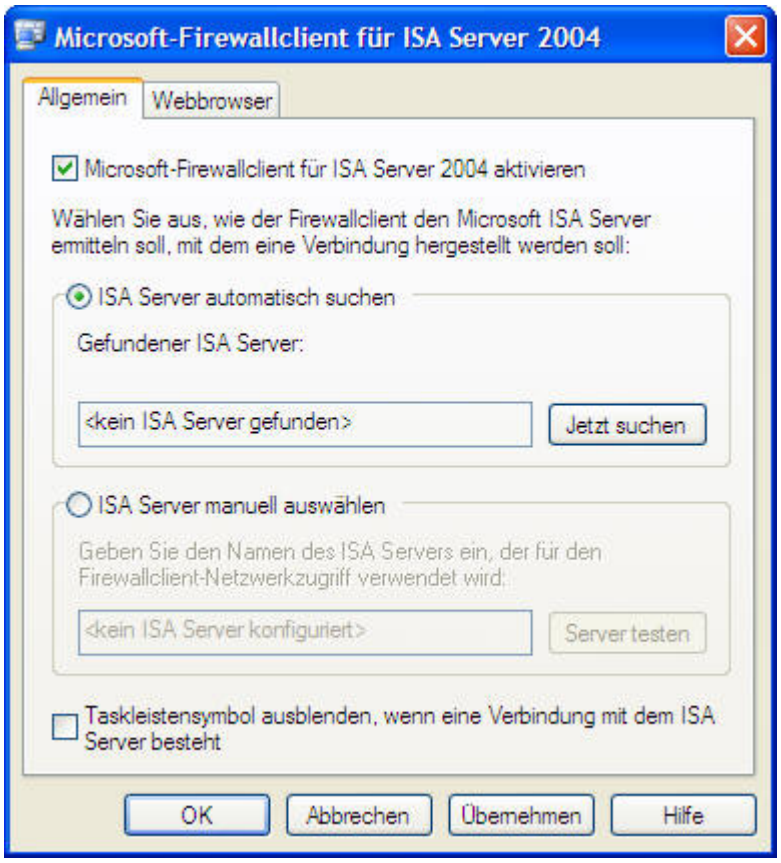
In den Eigenschaften der LAN-Einstellungen (IE -> Extras -> Internetoptionen -> Verbindungen) muss das Kontrollkästchen bei "Automatische Suche der Einstellungen" aktiviert sein. Bei einer Standard-Installation des IE ist dies der Fall.



Von nun an sucht sich der Client die Proxyeinstellungen selber. Erfahrungsgemäß kann dies beim ersten Aufruf des Browsers einige Sekunden dauern. Die automatische Suche kann auch für den Browser des ISA Computers selber verwendet werden.

6. Konfiguration des Firewallclients für die Automatische Suche

Natürlich unterstützt auch der Firewallclient die automatische Suche. Sobald der Client installiert ist müssen lediglich folgender Haken gesetzt werden:

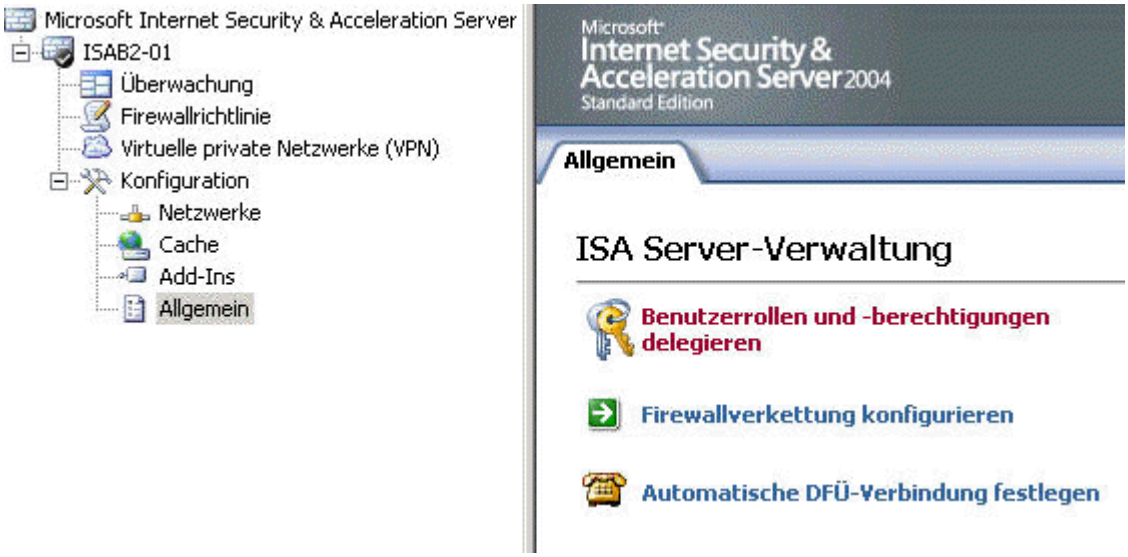

Microsoft-Firewallclient für ISA Server 2004
Allgemein
Webbrowser
Microsoft-Firewallclient für ISA Server 2004 aktivieren
Wählen Sie aus, wie der Firewallclient den Microsoft ISA Server ermitteln soll, mit dem eine Verbindung hergestellt werden soll:
ISA Server automatisch suchen
Gefundener ISA Server:
<kein ISA Server gefunden>
Jetzt suchen
ISA Server manuell auswählen
Geben Sie den Namen des ISA Servers ein, der für den Firewallclient-Netzwerkzugriff verwendet wird:
<kein ISA Server konfiguriert>
Server testen
Taskleistensymbol ausblenden, wenn eine Verbindung mit dem ISA Server besteht
OK
Abbrechen
Übernehmen
Hilfe

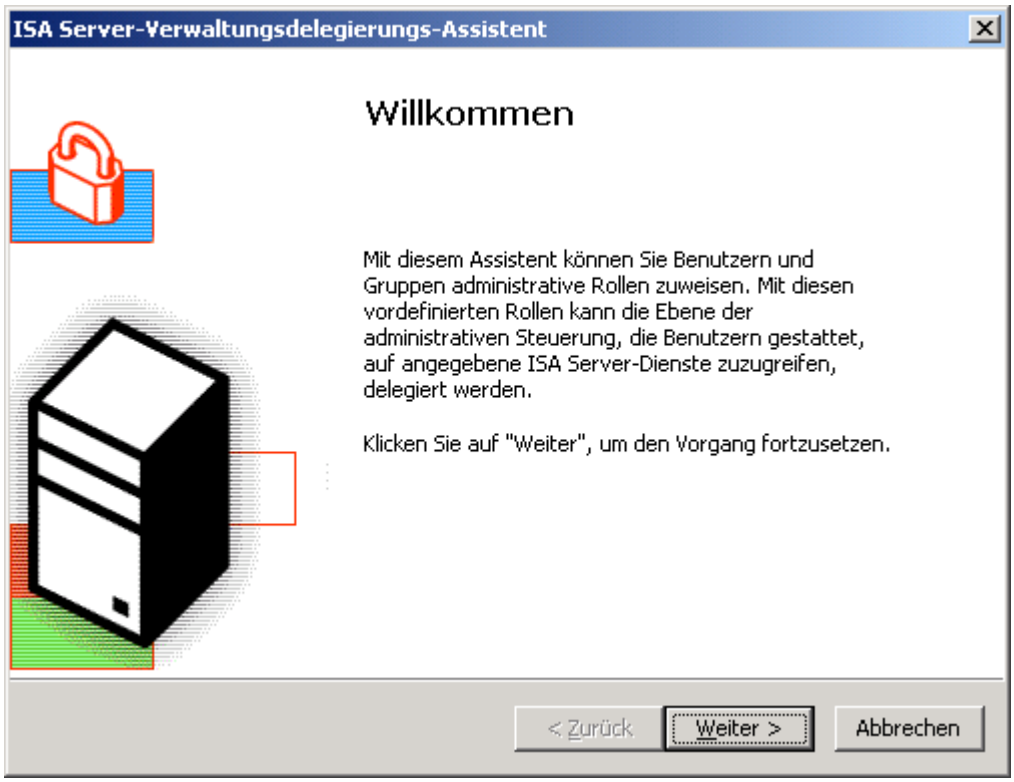
Benutzerrollen und -berechtigungen delegieren

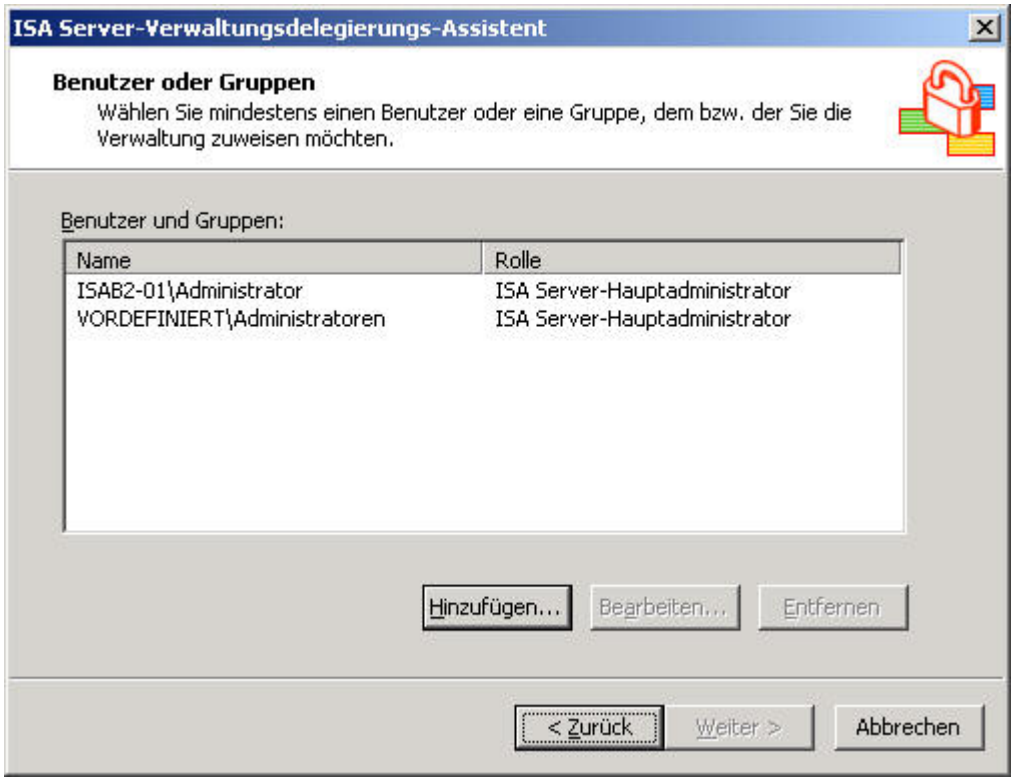
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Manchmal ist es notwendig, einem zusätzlichen Benutzer bestimmte Rechte für die ISA Server Verwaltung zu geben, ohne ihm gleich lokale Windows-Administrationsrechte zu vergeben. Genau dafür bietet der ISA Server 2004 die Option "Benutzerrollen und -berechtigungen delegieren" an. Zu finden ist sie in der ISA MMC unter Konfiguration -> Allgemein:



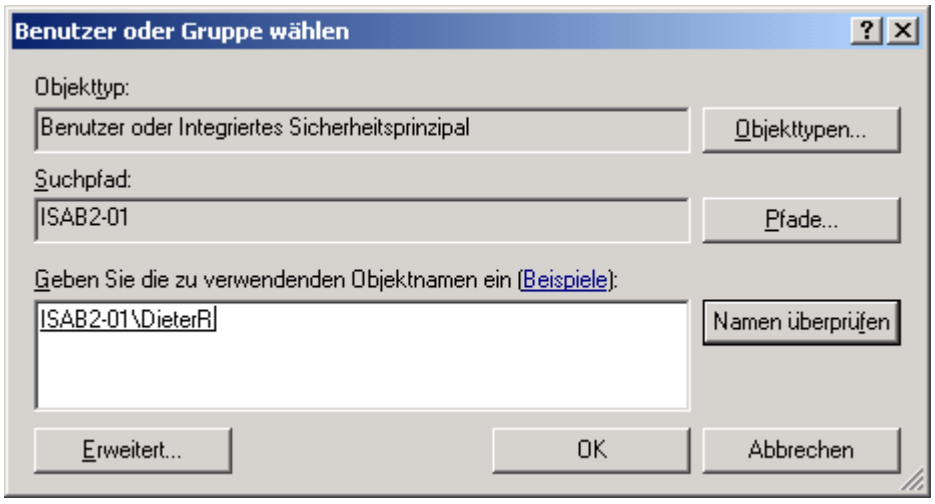


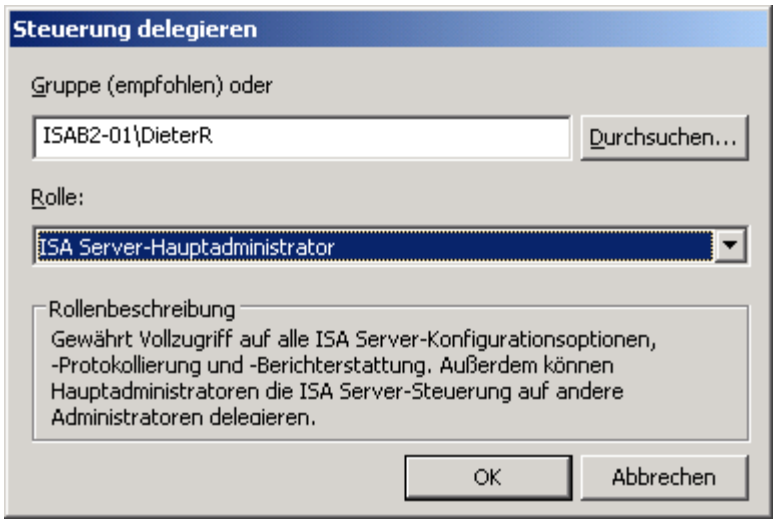


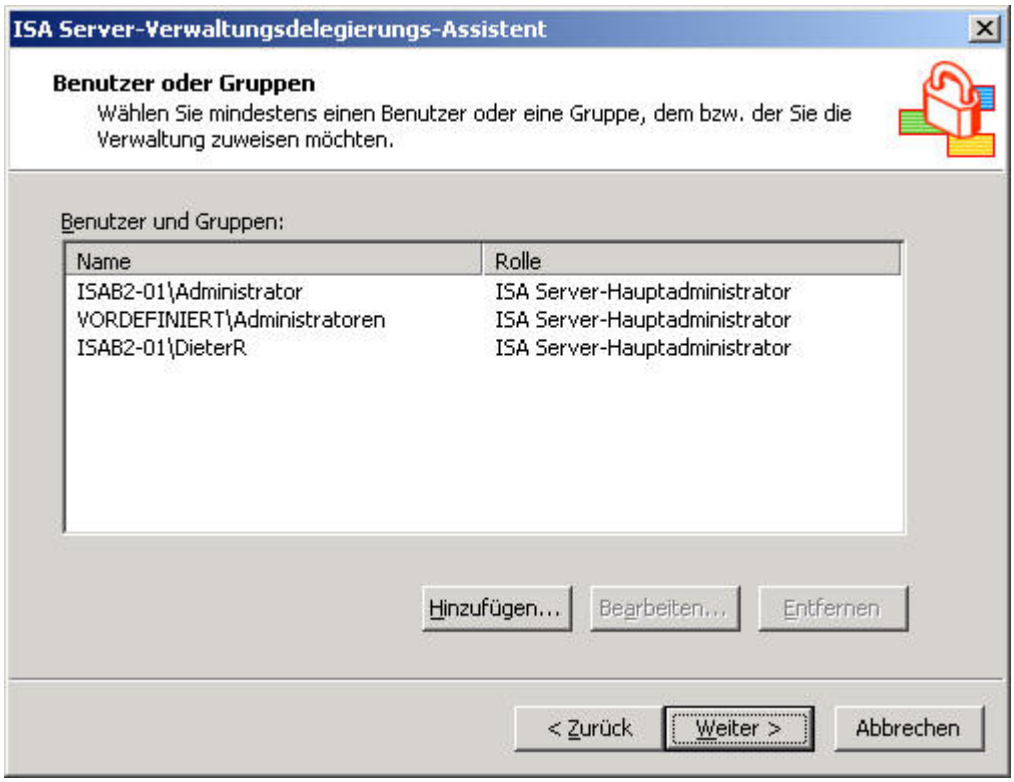
Folgende Rollen stehen zur Verfügung:

- ISA Server-Hauptadministrator:
  Gewährt Vollzugriff auf alle ISA Server-Konfigurationsoptionen, -Protokollierung und -Berichterstattung. Außerdem können Hauptadministratoren die ISA Server-Steuerung auf andere Administratoren delegieren.

- ISA Server-Basisüberwachung:
  Gewährt Zugriff auf die ISA Server-Basisüberwachungsfunktionen.
- Erweiterte ISA Server-Überwachung
  Gewährt Vollzugriff auf die gesamt ISA Server-Überwachung und Lesezugriff auf die ISA Server-Konfiguration.



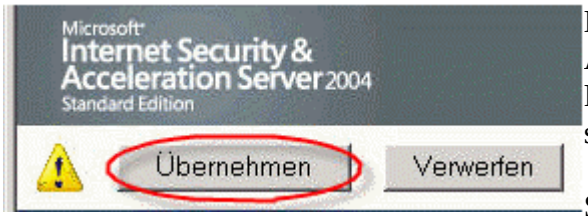




Nachdem ein Benutzer hinzugefügt wurde, erscheint eine Zusammenfassung:

Empfohlen wird statt eines einzelnen Benutzers eine Gruppe zu verwenden. Prinzipiell sollten Berechtigungen nur auf Gruppenebene statt auf Benutzerebene vergeben werden. Dies betrifft nicht nur die ISA Konfiguration; vielmehr die Filesystem- und Exchangerechte. Gruppen sind wesentlich flexibler handhabbar - ohne Aufwand kein ein Benutzer hinzugefügt werden, in dem er Mitglied der Gruppe wird. Schon hat er sämtliche benötigten Rechte. Wenn jedes Mal Rechte für einen einzelnen Benutzer vergeben werden müssten, wäre der Verwaltungsaufwand zu hoch und es kann leichter passieren, dass vergessen wird, einem Benutzer bei Bedarf Rechte zu entziehen (z.B. wenn sich seine Funktion geändert hat).

Tip: Die Zusammenfassung kann per Copy und Paste herausgenommen werden und in eine Dokumentation eingefügt werden. So spart man sich ggfs. Tipparbeit....



Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

Backup und Restore eines ISA Server 2004

Die Informationen in diesem Artikel beziehen sich auf:

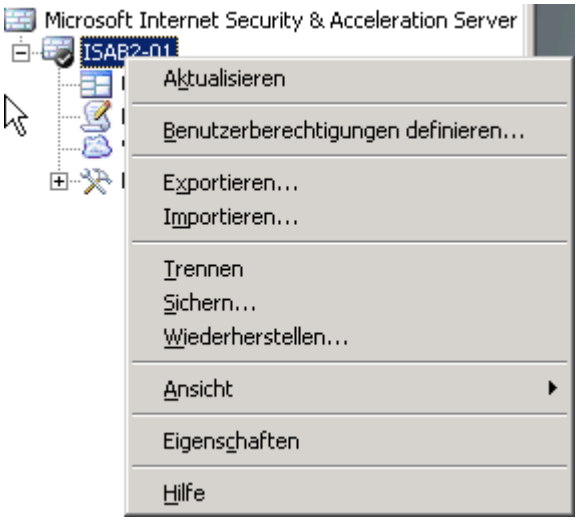
- Microsoft ISA Server 2004

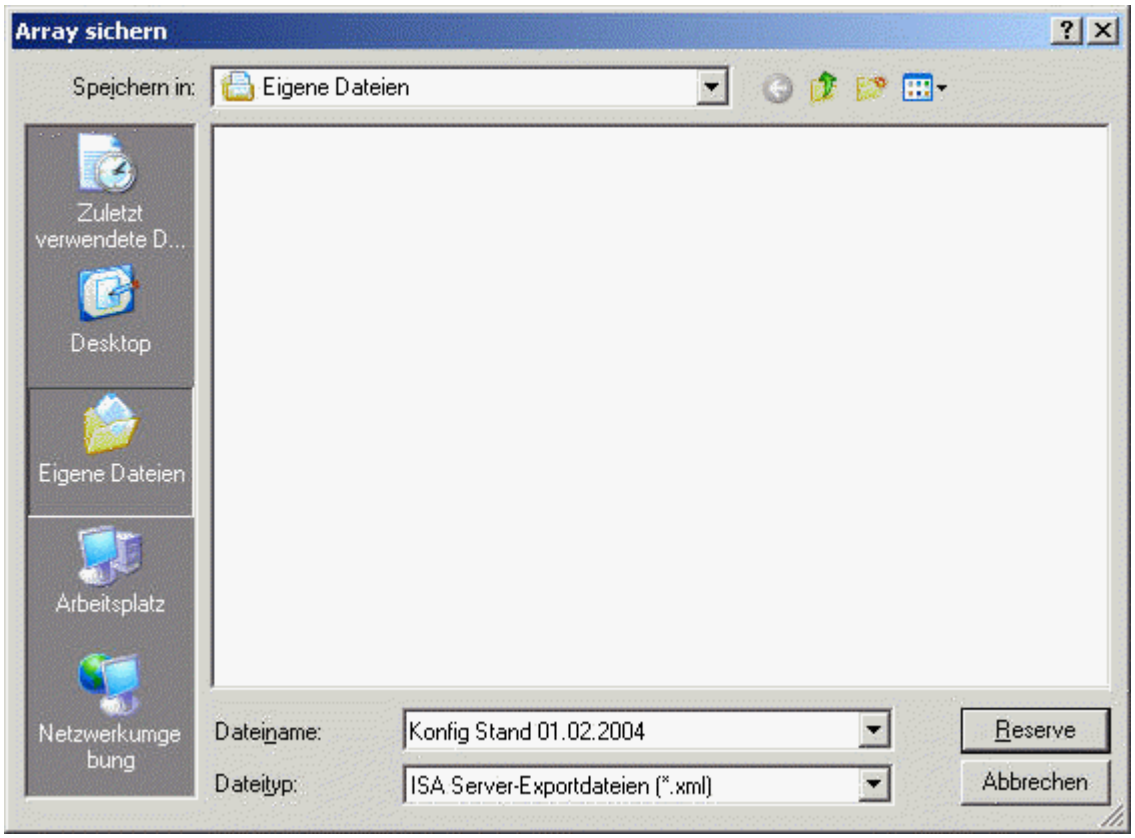
Das Backup der ISA Server-Konfiguration sollte eine Selbstverständlichkeit sein, zumal der ISA eine wesentliche und wichtige Komponente einer Netzwerkinfrastruktur darstellt. Aus diesem Grund enthält die ISA Verwaltungskonsole eine Sicherungs- und Wiederherstellungsfunktion. Damit können die Konfigurationsdaten in einer xml-Datei (lokal oder auf einem Netzwerklaufwerk) gespeichert werden.

Diese Sicherung enthält jedoch nicht alle Daten, die zur kompletten Wiederherstellung eines ISA Server Computers benötigt werden, sie sind lediglich ein Teil davon. Alle allgemeinen ISA-Konfigurationsinformationen werden gesichert. Für die Wiederherstellung nach einem Systemausfall wird außerdem die Sicherung der gesamten Computerkonfiguration benötigt! Deshalb sollte ein regelmäßiges Backup der Systemdaten erfolgen. Das ISA-eigene Backup kann nicht automatisiert werden. Die ISA Konfiguration sollte jedesmal vor- und nach Änderungen der Einstellungen durchgeführt werden.

Die Sicherungs-/Wiederherstellungsfunktion kann NICHT dazu verwendet werden, die Konfiguration eines ISA Servers auf einen anderen zu übertragen (clonen). Verwenden Sie dazu die Export-/Importfunktionalität des ISA Servers.

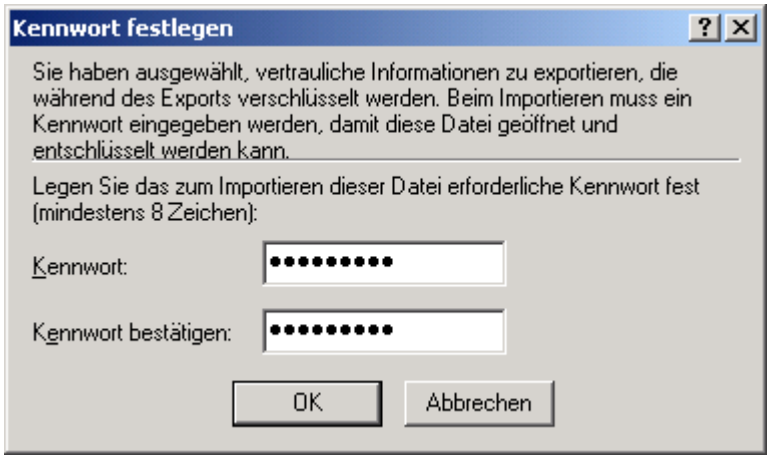
1. Backup



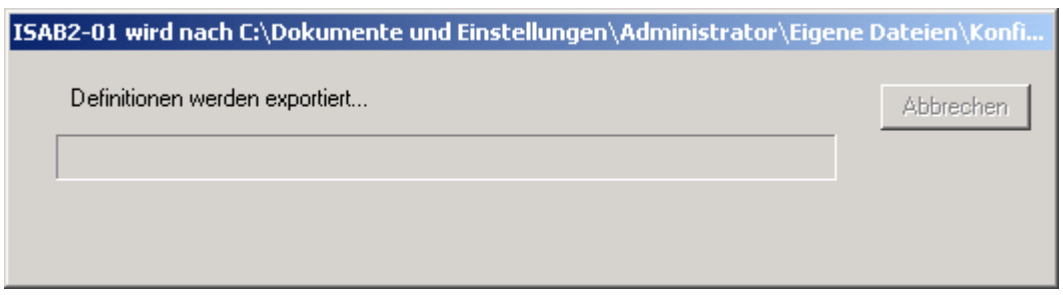


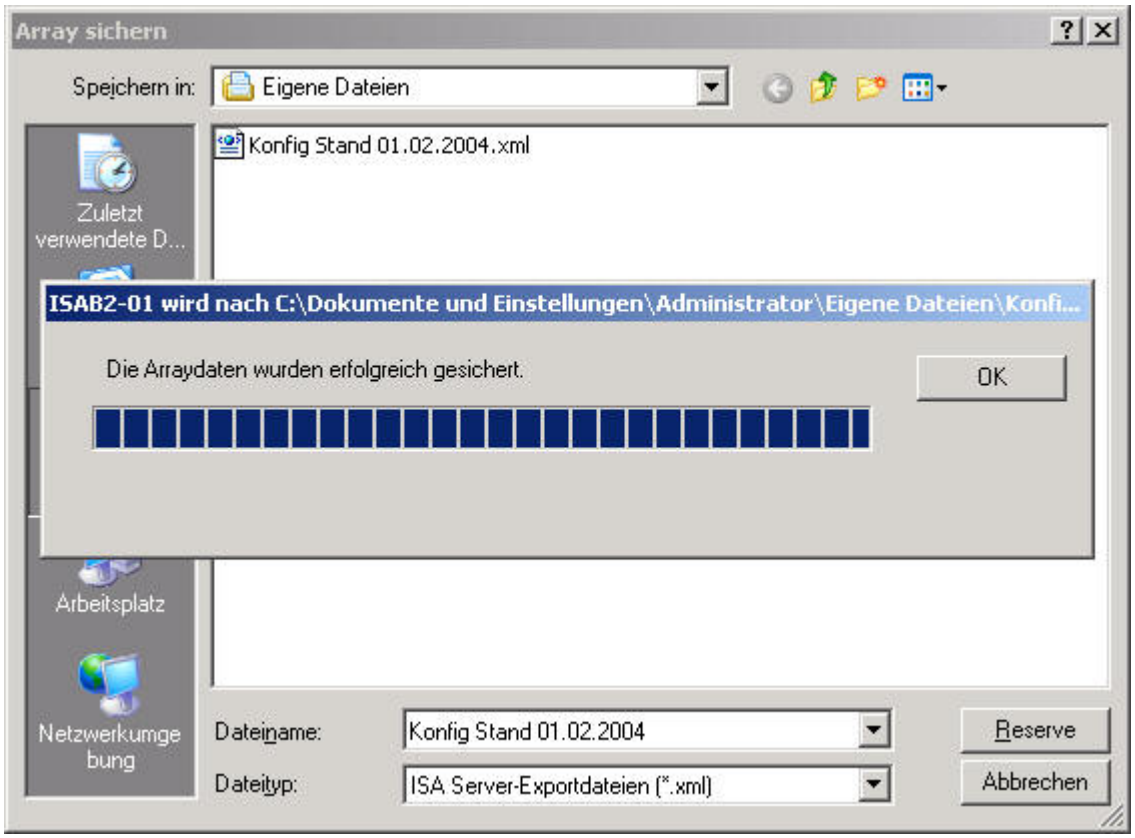
Geben Sie einen beschreibenden Namen der Sicherungsdatei an.

Die xml-Datei wird teilweise verschlüsselt, deshalb muss ein Kennwort vergeben werden:



Das Sichern der Konfiguration dauert nur wenige Sekunden



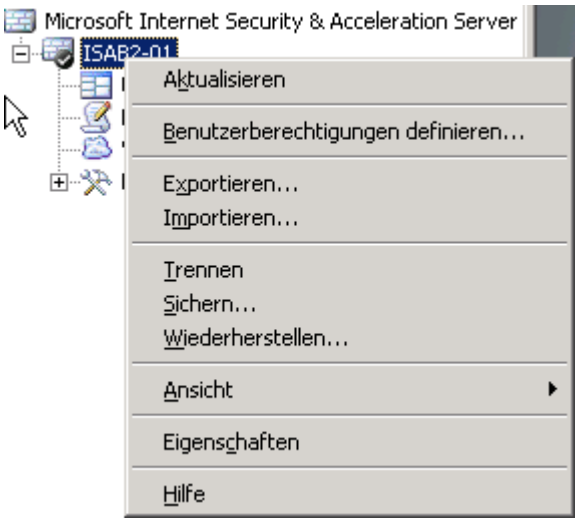


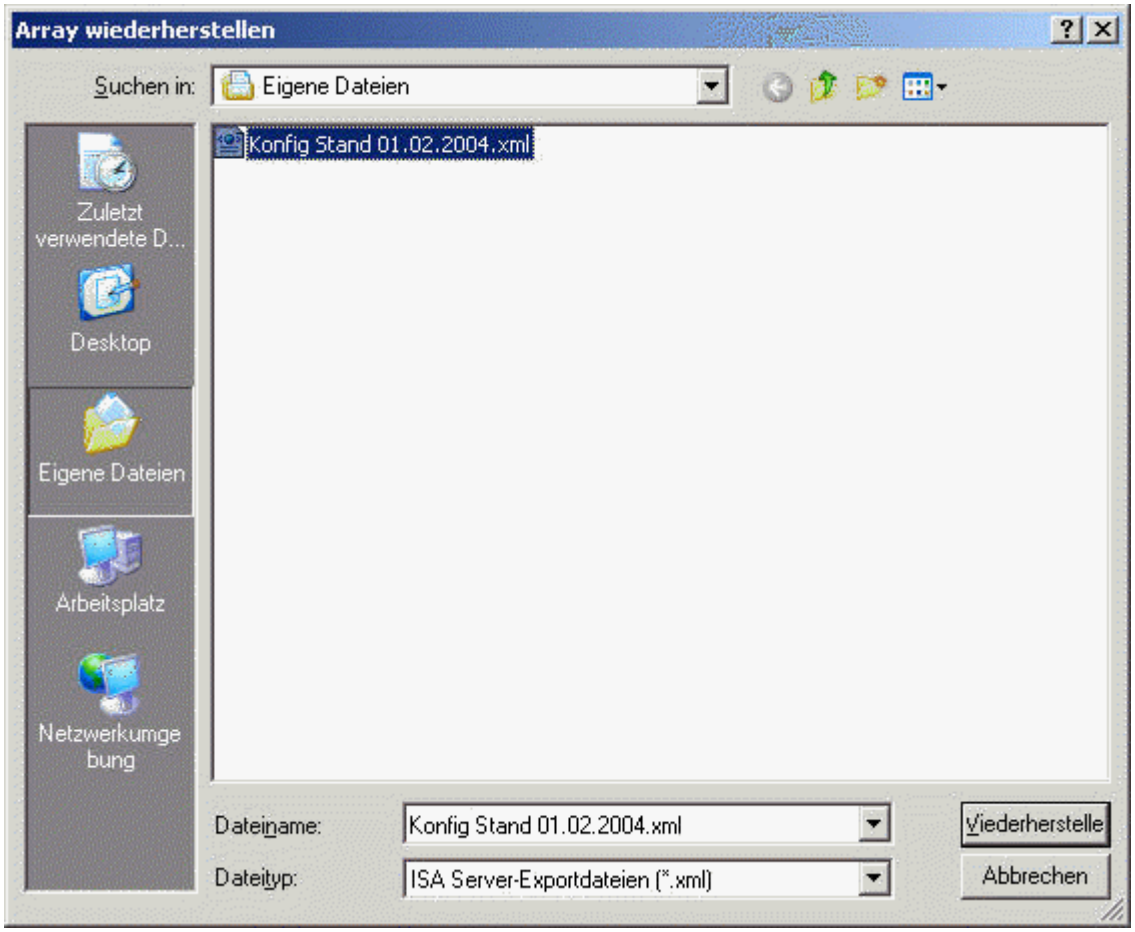
Hier ein kleiner Auszug aus der soeben erzeugten Sicherungsdatei:

```
    <fpc4:Name dt:dt="string">DHCP(Anforderung)</fpc4:Name>
    <fpc4:Predefined dt:dt="boolean">1</fpc4:Predefined>
    <fpc4:ProtocolCategory dt:dt="int">4</fpc4:ProtocolCategory>
    <fpc4:Refs StorageName="ApplicationFilters" StorageType="1" />
  - <fpc4:ProtocolConnections StorageName="PrimaryConnections"
     StorageType="1">
    - <fpc4:ProtocolConnection StorageName="{1e24fd7c-7b32-4f58-8e0e-
       3fdd297d891c}" StorageType="1">
       <fpc4:ConnectionType dt:dt="int">17</fpc4:ConnectionType>
       <fpc4:Direction dt:dt="int">1</fpc4:Direction>
       <fpc4:PortHigh dt:dt="int">67</fpc4:PortHigh>
       <fpc4:PortLow dt:dt="int">67</fpc4:PortLow>
     </fpc4:ProtocolConnection>
    </fpc4:ProtocolConnections>
  </fpc4:Protocol>
- <fpc4:Protocol StorageName="{a3244b59-ca48-4619-8163-0b65676bd959}"
    StorageType="1">
    <fpc4:Components dt:dt="int">16</fpc4:Components>
    <fpc4:Guid dt:dt="string">{a3244b59-ca48-4619-8163-0b65676bd959}
     </fpc4:Guid>
```

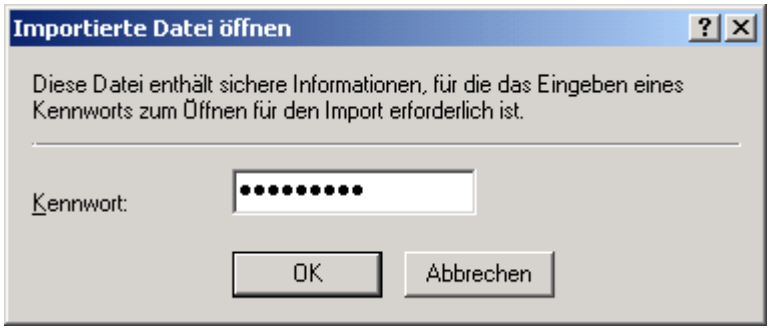
2. Restore

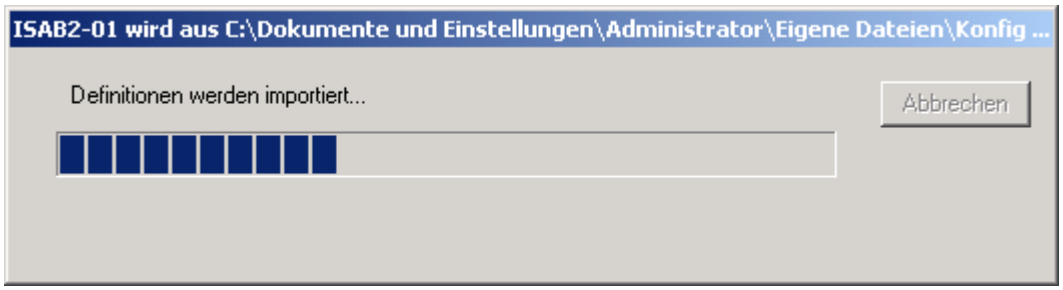
Für ein Restore ist der Weg nahezu identisch:

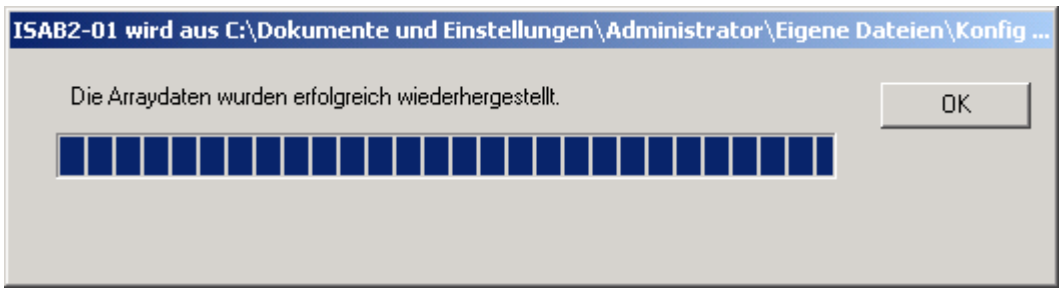




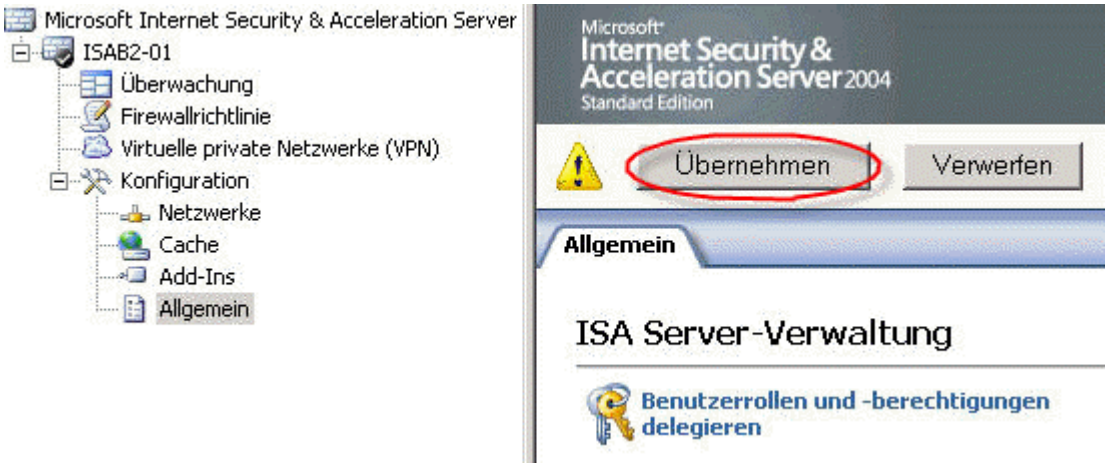
Wählen Sie die wiederherzustellende Datei aus und geben Sie das Kennwort ein.







Damit die Änderungen wirksam werden, müssen sie übernommen werden:



Nun hat dieser ISA Server wieder den Stand zum Zeitpunkt der Erstellung der Sicherungsdatei.

Remoteverwaltung eines ISA Server 2004: Teil 1 - Remotedesktop (RDP)

Die Informationen in diesem Artikel beziehen sich auf:

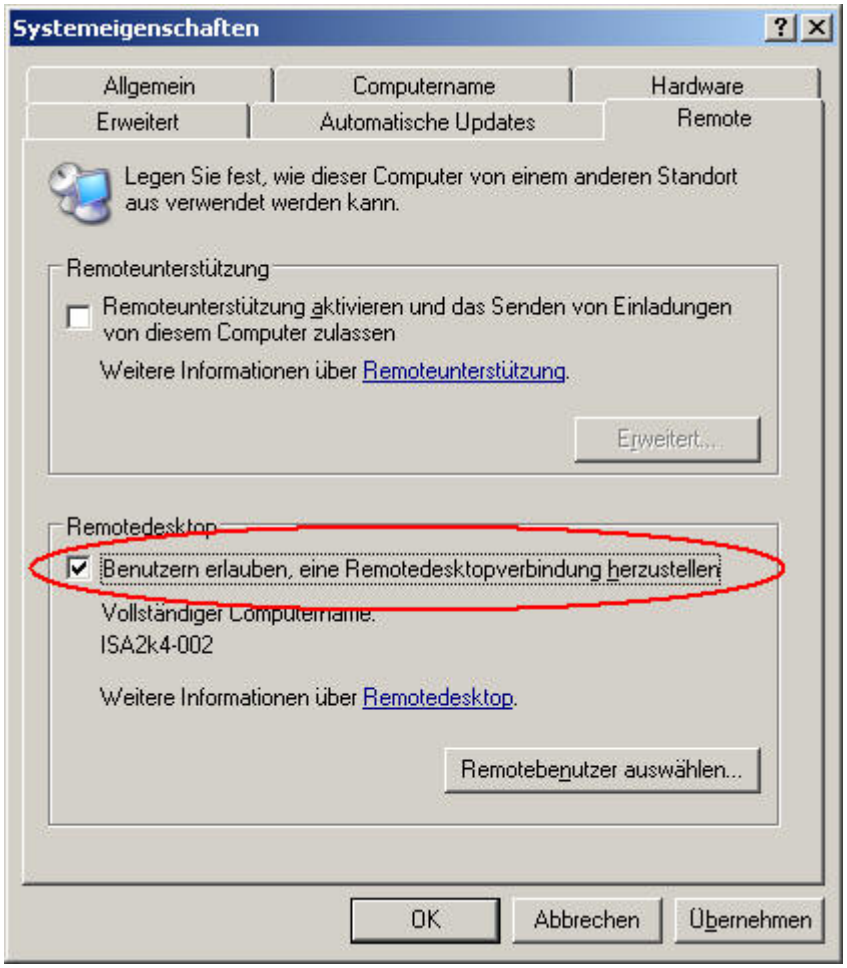
- Microsoft ISA Server 2004

Zur Verwaltung und Konfiguration des ISA Server 2004 wird beim normalen Setup auch die Managementkonsole mitinstalliert. Klassischerweise administriert man den ISA Server direkt an der Maschine, auf der er auch installiert ist. Jedoch gibt es häufig Situationen, in denen dieser Administrationszugang zur Verfügung steht oder nicht gewünscht wird. Z.B. Wenn der ISA Server in einem Rechenzentrum oder einem anderen Standort steht. Genau deshalb gibt es (natürlich) die Möglichkeit, den ISA Server fernzuverwalten. Es stehen zwei unterschiedliche Methoden zur Verfügung: Remote Desktop und Managementkonsole.

Einrichten des ISA Servers zur Fernverwaltung mittels Remotedesktop (RDP):

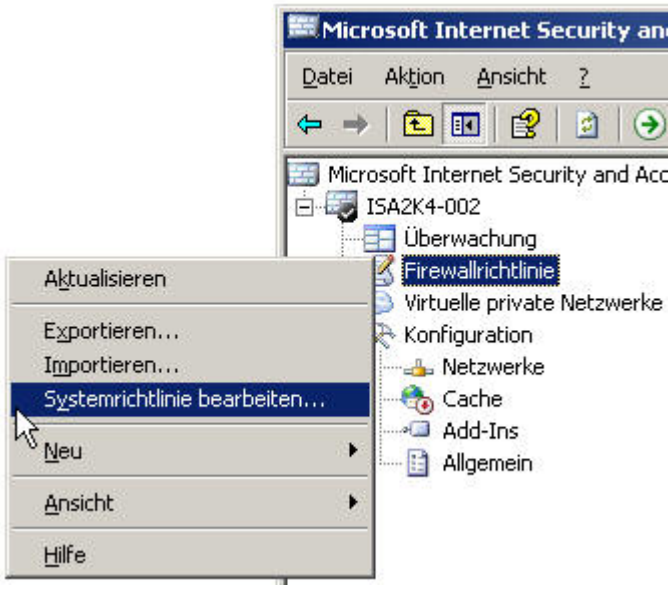
Um den ISA Server über die Remotedesktop-Funktionalität von Windows Server 2003 (bei Windows 2000 Server ist es das selbe Prinzip, die Technik heißt dort jedoch noch "Terminaldienst im Administrationsmodus") verwalten zu können müssen sowohl am Windows Server als auch in der ISA Verwaltung kleine Konfigurationsschritte durchgeführt werden.

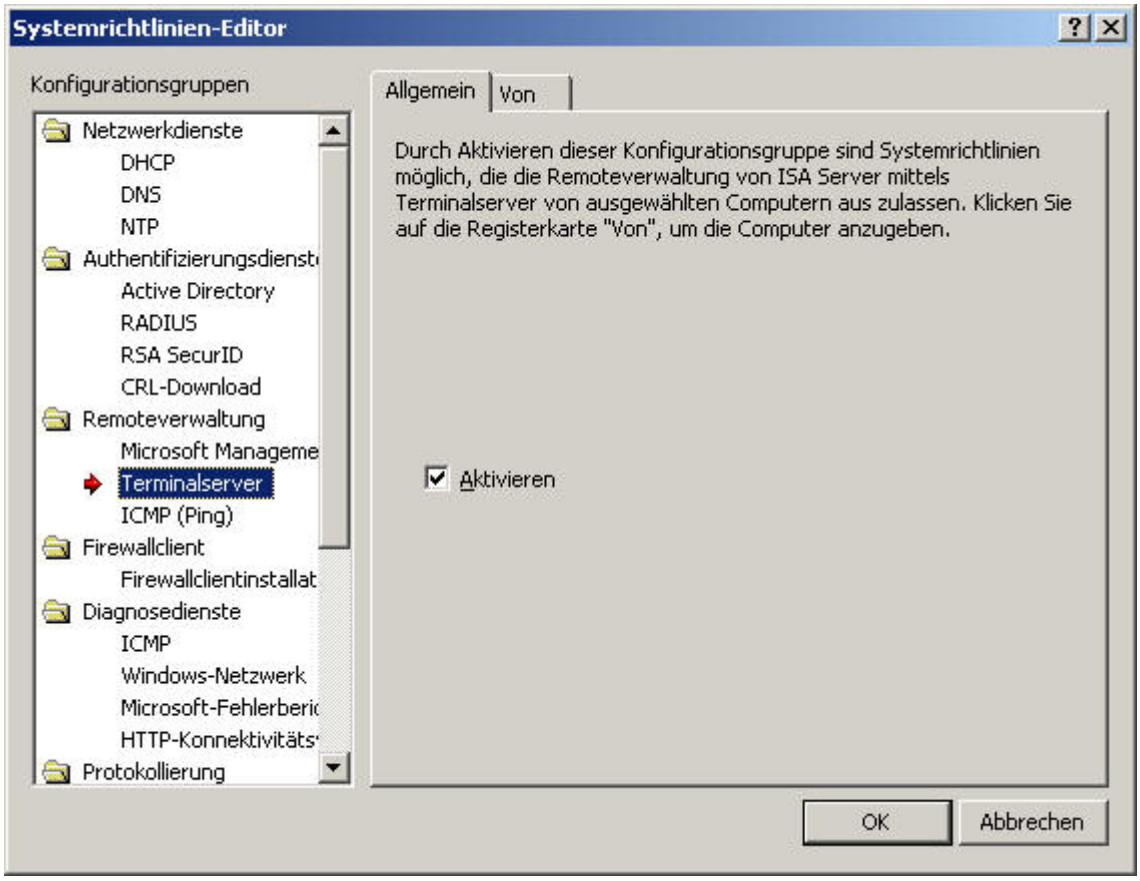
Zuerst muss der Windows Server zulassen, dass er über RDP verwaltet werden kann:



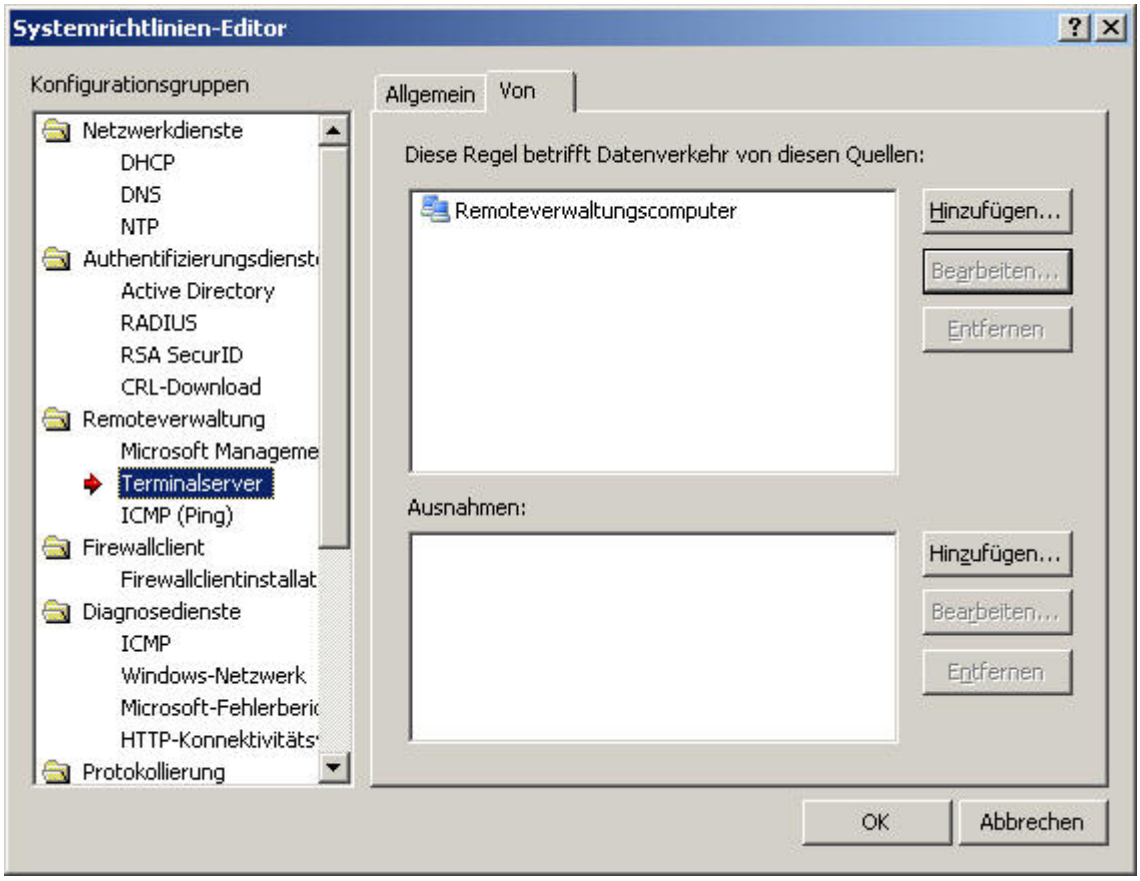
In den Systemeigenschaften (Systemsteuerung -> System) muss auf der Registerkarte "Remote" der Remotedesktop aktiviert werden. Standardmäßig dürfen dann nur (lokale) Administrationen eine RDP-Verbindung herstellen. Man kann aber jederzeit weitere berechtigte Benutzer hinzufügen.

Anschließend muss im ISA Server die Systemrichtlinie für Remoteverwaltung aktiviert/angepasst werden:

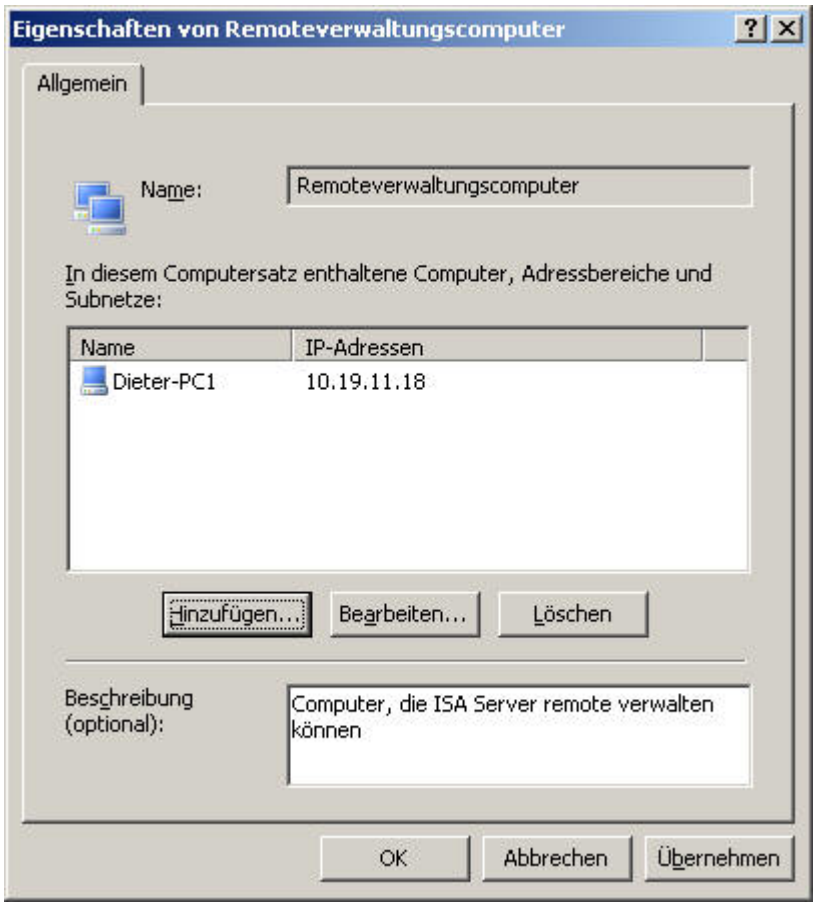


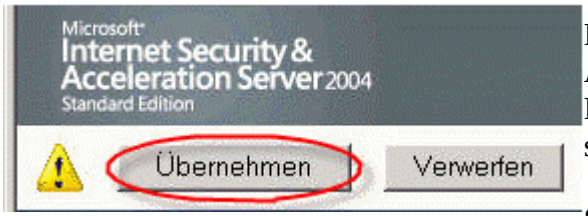


Hier muss der Haken gesetzt sein. Anschließend sollte man sicherstellen, dass in der Registerkarte "Von" nur ein Computerset enthalten ist, welches wiederum nur die berechtigten Rechner beinhaltet:



Man kann gleich hier berechtigte Computer der Gruppe "Remoteverwaltungscomputer" hinzufügen. Es empfiehlt sich, in dieser Gruppe gleich alle Rechner hinzuzufügen, die später sowohl über RDP als auch die MMC auf die ISA Server Einstellungen zugreifen sollen.





Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

Mit diesem Konfigurationsschritt hat der ISA Server eine Richtlinie gesetzt, die allen Computern in der Gruppe "Remoteverwaltungscomputer" den Zugang über RDP erlaubt. Dabei ist es unerheblich, ob ein Client der Gruppe "Remoteverwaltungscomputer" eine interne oder eine externe IP-Adresse hat. Selbst eine Mischung aus internen/externen Clients ist zulässig. Dadurch kann auch der Remotedesktop des ISA Server Computers für bestimmte externe Clients veröffentlicht werden. Beachten Sie jedoch, dass bei Angabe eines externen Clients dieser automatisch auch alle Zugriffsrechte erhält, die der Remoteverwaltungscomputergruppe zugeteilt wurden. In den meisten Situationen werden das zu viele Rechte sein und es ist wünschenswert, dem externen Client *wirklich* nur den Remotedesktop zur Verfügung zu stellen. Diese Richtlinie wird im Artikel Lokaler Remotedesktop beschrieben.

Vom Client aus ruft man einfach die "Remotedesktopverbindung" (Start -> Programme -> Zubehör -> Kommunikation) auf (alternativ: `mstsc`) und gibt den Namen oder die IP-Adresse des ISA Servers ein:

Tip: Mit dem Befehl `mstsc /console` ruft man eine Remotedesktopverbindung auf die Konsole auf. Das hat mehrere Vorteile:

- *man sieht Popups/Warnungen*
- *man kann meist Software installieren, die nicht im Terminalmodus installiert werden kann*
- *man kann die Konsole so übernehmen/übergeben wie man sie am "echten" Monitor sieht*

Remoteverwaltung eines ISA Server 2004: Teil 2 - Managementkonsole (MMC)

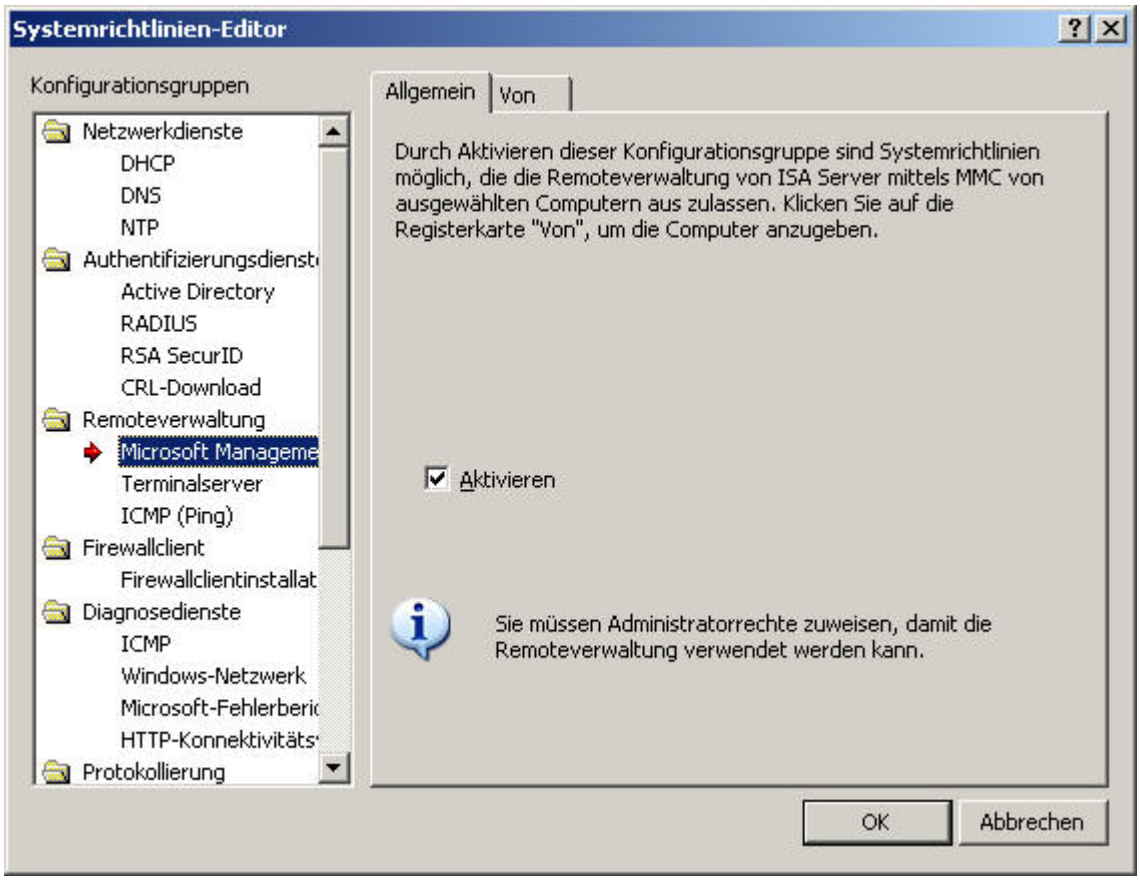
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

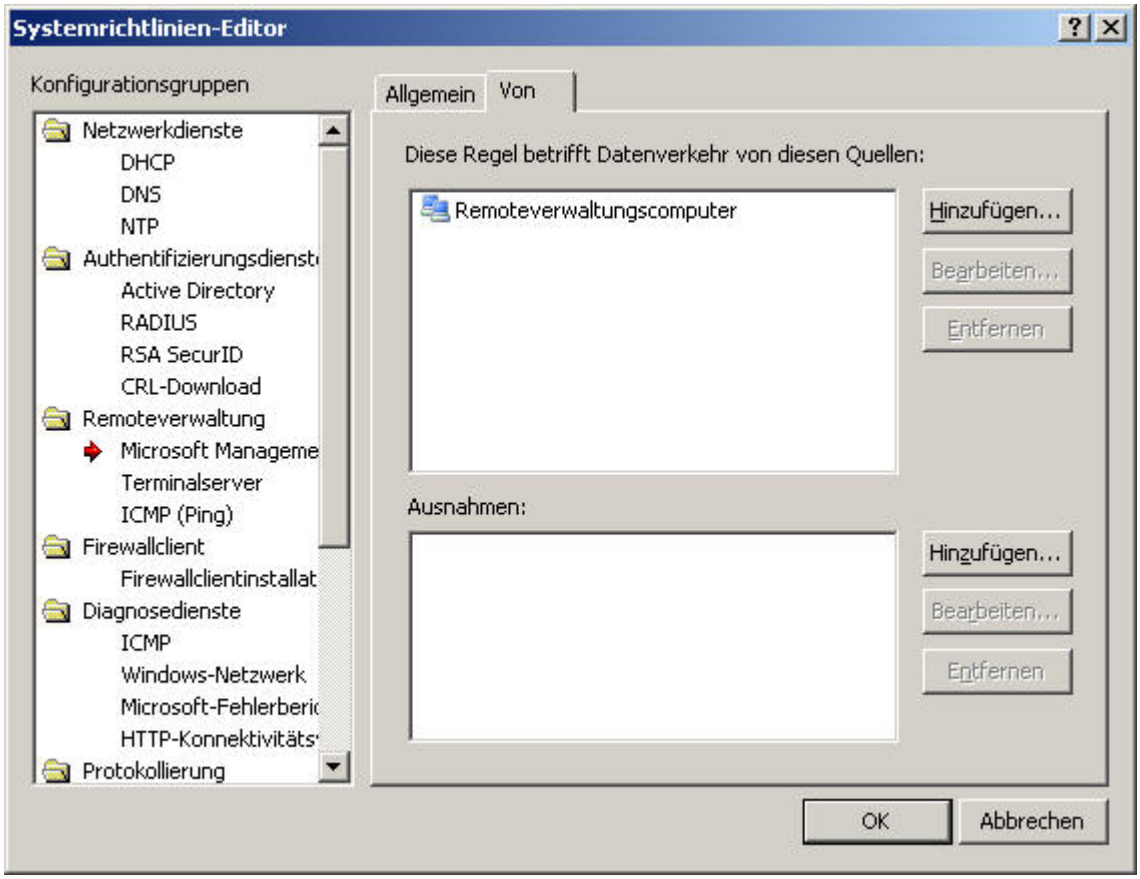
Zur Verwaltung und Konfiguration des ISA Server 2004 wird beim normalen Setup auch die Managementkonsole mitinstalliert. Klassischerweise administriert man den ISA Server direkt an der Maschine, auf der er auch installiert ist. Jedoch gibt es häufig Situationen, in denen dieser Administrationszugang zur Verfügung steht oder nicht gewünscht wird. Z.B. Wenn der ISA Server in einem Rechenzentrum oder einem anderen Standort steht. Genau deshalb gibt es (natürlich) die Möglichkeit, den ISA Server fernzuwarten. Es stehen zwei unterschiedliche Methoden zur Verfügung: Remote Desktop und Managementkonsole.

Einrichten des ISA Servers zur Fernverwaltung mittels Managementkonsole (MMC):

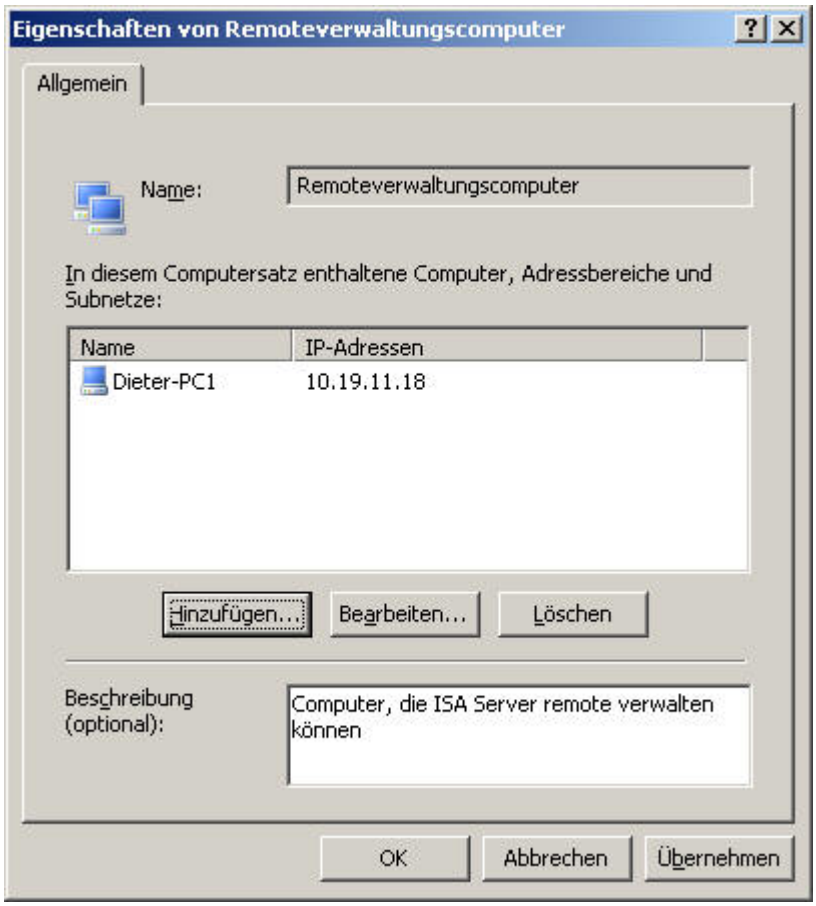
Die Vorbereitungen des ISA Servers zur Fernkonfiguration über die MMC ähnelt der Konfig für RDP. Es muss wieder eine Systemrichtlinie angepasst werden:

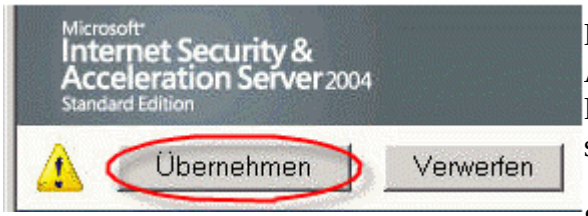


Hier muss der Haken gesetzt sein. Anschließend sollte man sicherstellen, dass in der Registerkarte "Von" nur ein Computerset enthalten ist, welches wiederum nur die berechtigten Rechner beinhaltet:



Man kann gleich hier berechtigte Computer der Gruppe "Remoteverwaltungscomputer" hinzufügen. Es empfiehlt sich, in dieser Gruppe gleich alle Rechner hinzuzufügen, die später sowohl über RDP als auch die MMC auf die ISA Server Einstellungen zugreifen sollen.



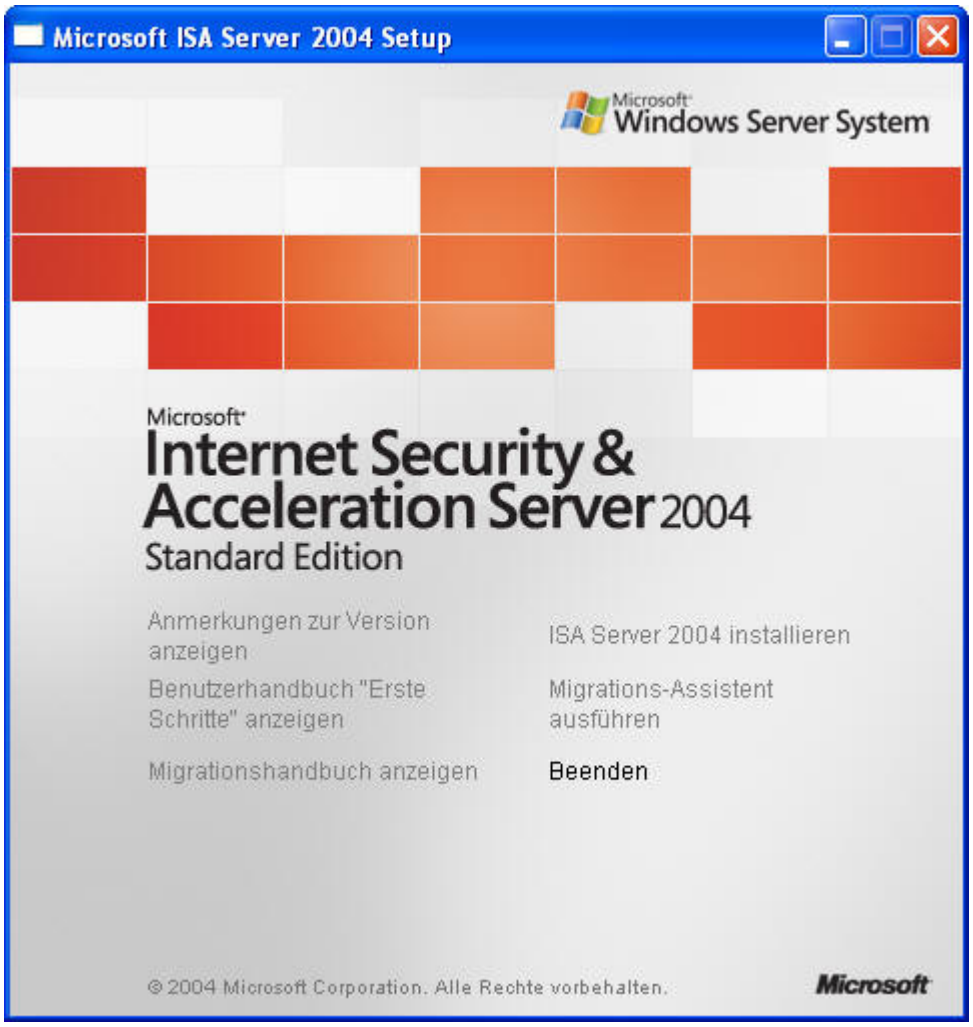


Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

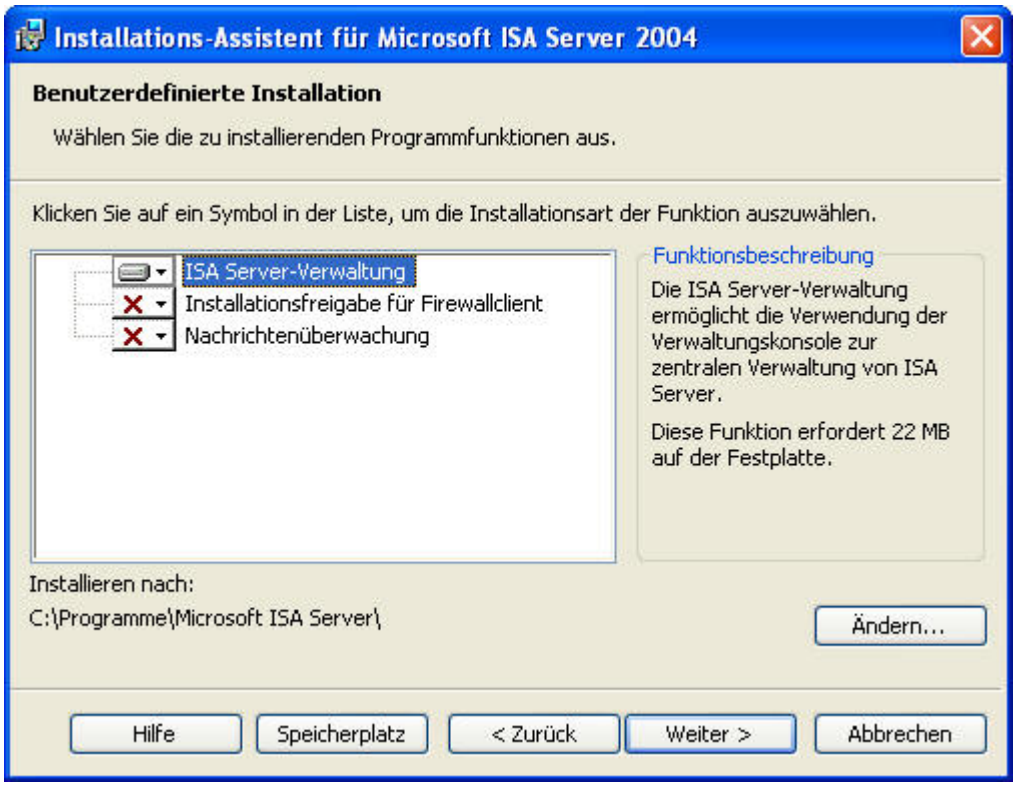
Mit diesem Konfigurationsschritt hat der ISA Server eine Richtlinie gesetzt, die allen Computern in der Gruppe "Remoteverwaltungscomputer" den Zugang über die MMC erlaubt.

Als nächstes muss die Managementkonsole auf dem Client installiert werden. Dazu ruft man wieder das Setup von der ISA Server CD auf.

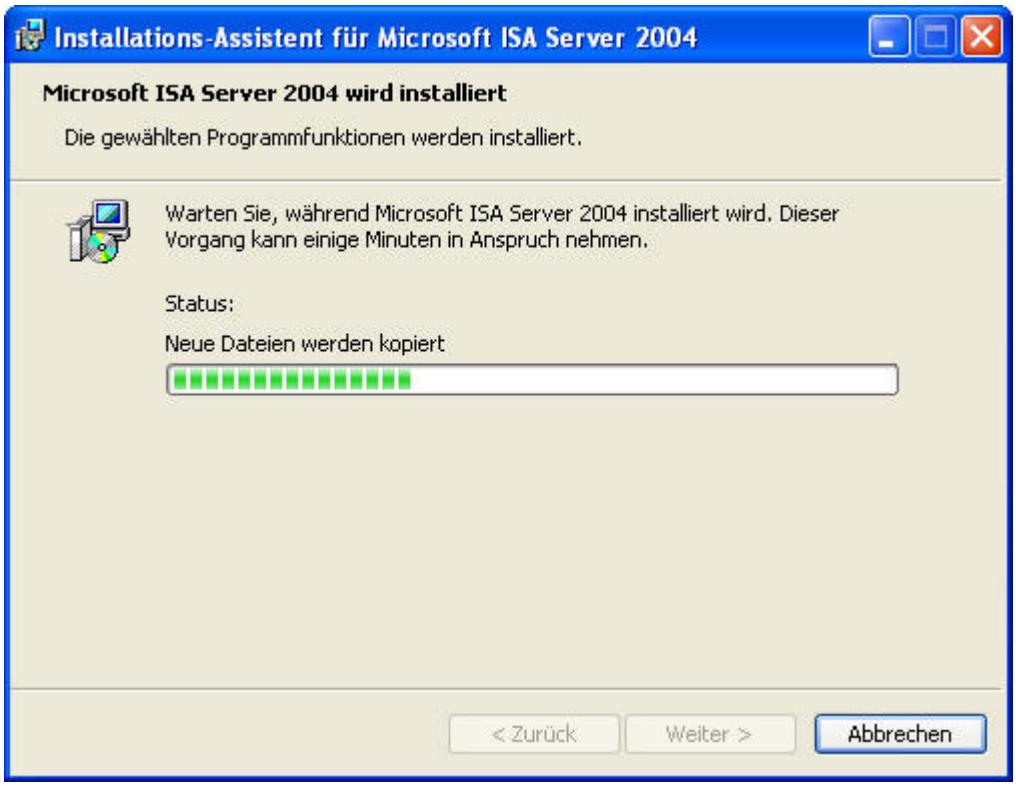


Hier bitte "ISA Server 2004 installieren" auswählen.

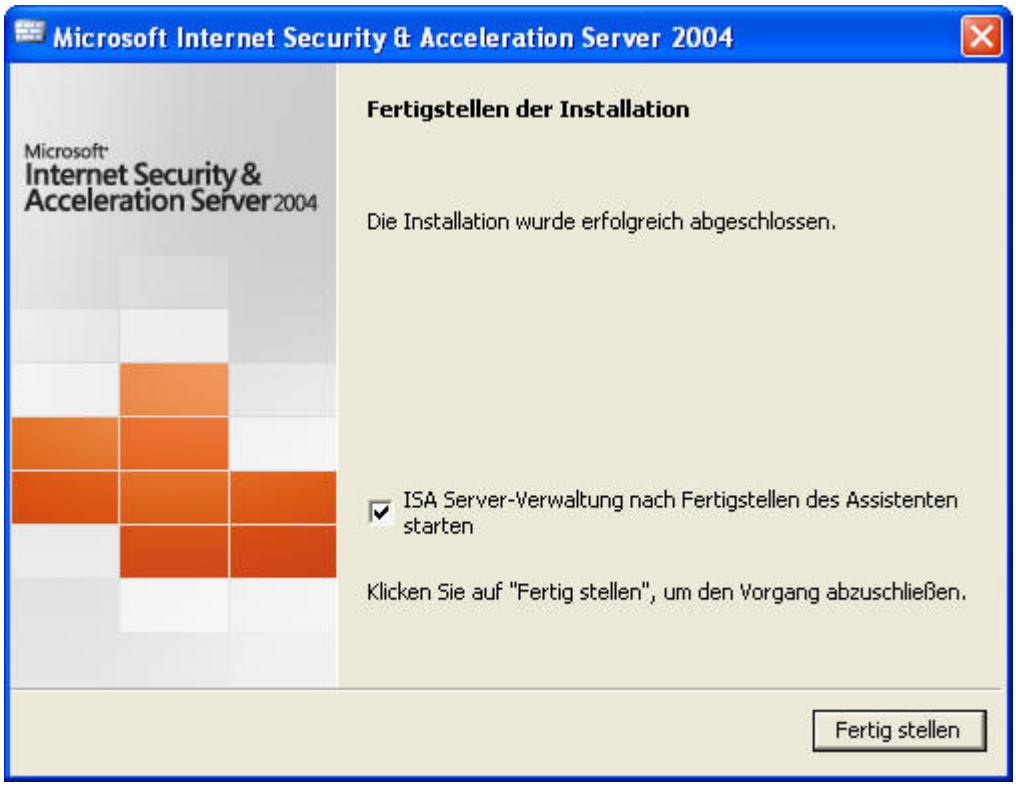
Nach akzeptieren der EULA und Eingabe der Lizenznummer gelangt man zum Auswahlmenü:



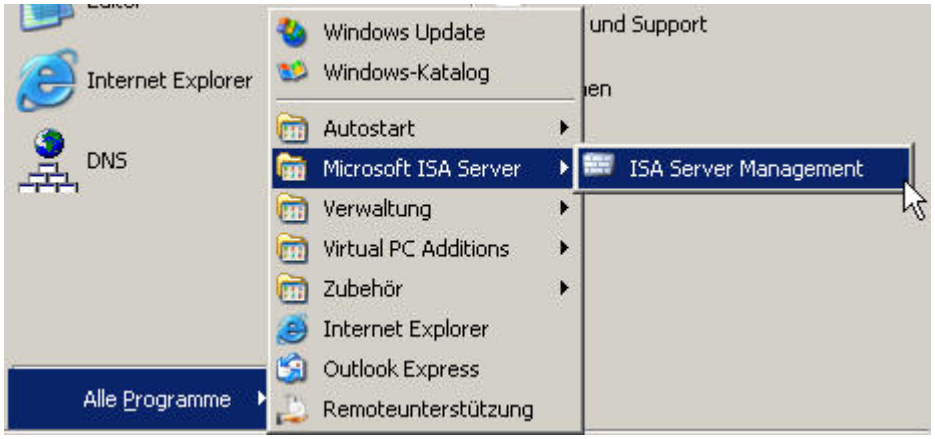
In vorliegenden Beispiel wird nur die ISA Server-Verwaltung installiert.



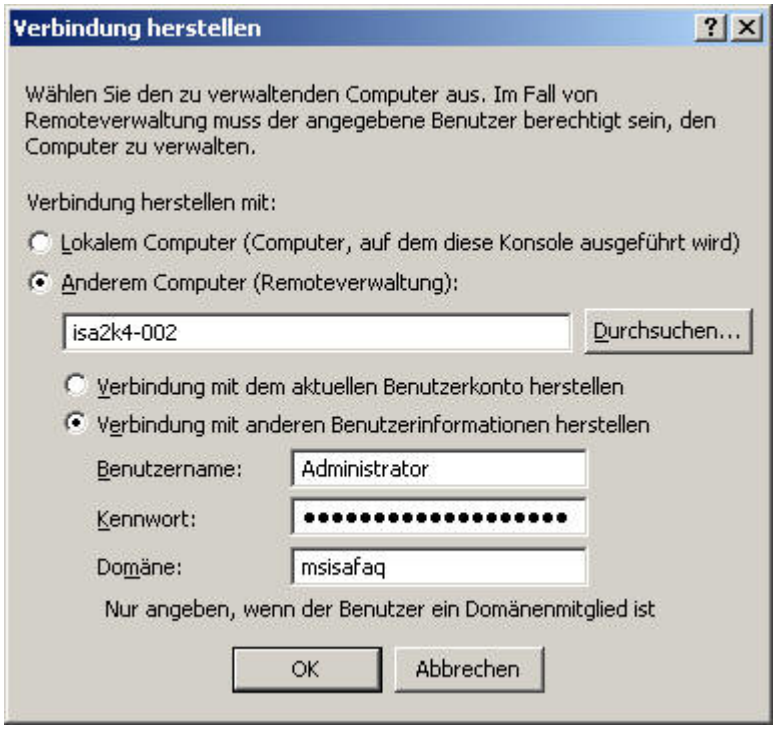
Nach kurzer Wartezeit ist die Installation fertig:



Nach der Installation steht im Startmenü der Eintrag "ISA Server Management" zur Verfügung:



Wird die Konsole zum ersten Mal geöffnet, muss eine Verbindung zum ISA Server hergestellt werden:



Wenn das Benutzerkonto des Benutzers, auf dessen Rechner die MMC installiert ist nicht über eine entsprechende Rolle/Berechtigung verfügt, kann hier ein berechtigtes Konto hinterlegt werden.

Nun kann der Benutzer entsprechend seiner Rolle Konfigurationsarbeiten durchführen.

Wichtig anzumerken ist noch, dass auf einem Rechner nur entweder die Managementkonsole für den ISA 2000 oder für den ISA 2004 installiert sein kann. Beide zusammen gehen leider nicht.

Aktuell installierte Produktversion herausfinden

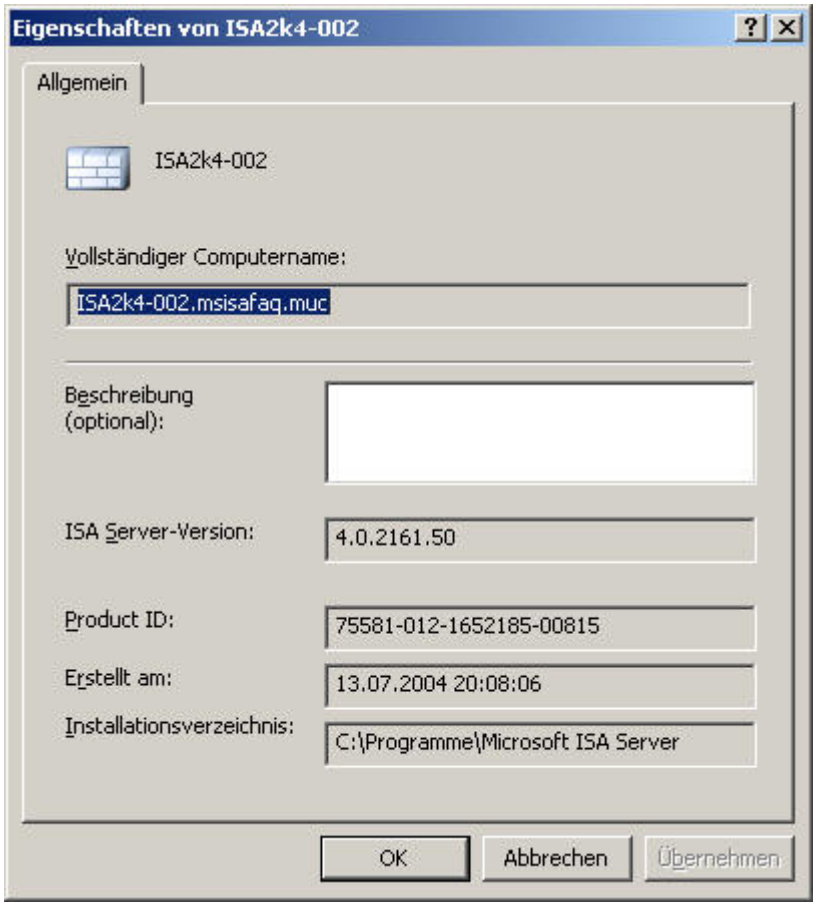
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Dass ein ISA Server 2004 installiert ist, wird dem Administrator sicherlich aufgefallen sein. Und solange es noch keine Hotfixe oder Servicepacks gibt, ist die installierte detaillierte Produktversion (=Bulidnummer) nicht von großer Bedeutung. Spätestens nach dem Erscheinen der ersten Erweiterung für den ISA oder zu Dokumentationszwecken ist es wesentlich zu wissen, welche genaue Version installiert ist. Das herauszufinden ist ganz einfach.

In der ISA Managementkonsole findet man unter dem Knoten "Allgemein" den Punkt

. Dort sind alle benötigten Informationen zu sehen:



Dieser Artikel wird nach Bedarf gepflegt und listet alle wesentlichen Versionsnummern auf.

4.0.2161.50	13.07.2004	RTM - Final Version
4.0.2141.50	07.04.2004	RC refresh
4.0.2076.50	24.02.2004	RC
4.0.1872.0	14.11.2003	Beta 2

Natürlich gab es vor der RTM Version noch wesentlich mehr verfügbare Builds. Die hier alle aufzulisten macht jedoch wenig Sinn.

ISA Info - >Das< Dokumentations- und Supporttool für den ISA Server 2004

Die Informationen in diesem Artikel beziehen sich auf:

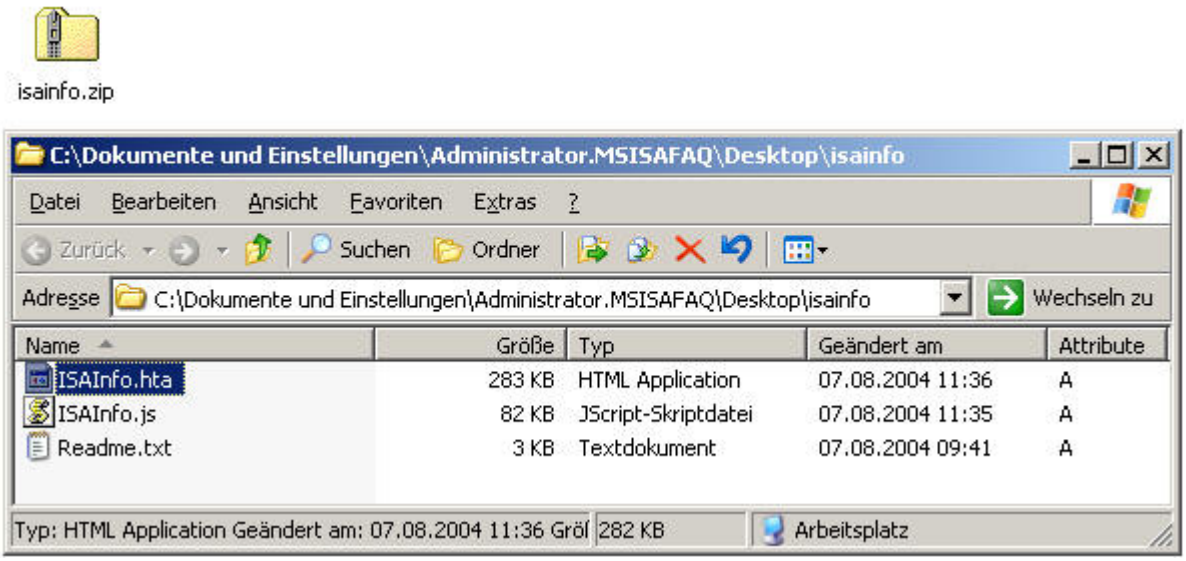
- Microsoft ISA Server 2004

Jim Harrison stellte bereits Ende 2001 eine Version von ISA Info für den ISA Server 2000 vor. Damit war zum ersten Mal ein Dokumentationstool verfügbar, welches sämtliche Einstellungen der ISA Konfiguration in ein Textfile exportierte. Mit diesem Infofile konnte z.B. der Support schnell wesentliche Informationen über das System bekommen oder man konnte es zur Netzwerkdokumentation verwenden.

Kurz nach Erscheinen des ISA Server 2004 ist auch eine angepasste Version von ISA Info verfügbar. Dank der XML-Unterstützung des ISA 2004 stehen hier mehr Möglichkeiten zur Verfügung. Auch diese Version eignet sich besonders zur Dokumentation oder für Supportzwecke.

Die jeweils aktuelle Version finden Sie hier.

Nach dem downloaden und entpacken des Zip-Files sind drei Dateien vorhanden:



- `Readme.txt` enthält neben den rechtlichen Hinweisen und Nutzungsrechten eine kurze Beschreibung der ISAInfo-Dateien.
- `ISAInfo.js` ist das Tool zum Sammeln der ISA 2004 Informationen. Es ist nicht mit ISA Server 2000 lauffähig. Dafür steht eine eigene Version zur Verfügung. Starten Sie das Tool vom ISA Server aus. Sollte der Windows Scripting Host nicht installiert sein, starten Sie das Tool mit `cscript isainfo.js`
  Durch den Export wurden zwei neue Dateien angelegt:

    - `ISAInfo2004_MachineName.xml`
      Dieses File beinhaltet alle ISA Konfigurationsdaten (erzeugt durch die ISA Backup-Routine) sowie darüber hinaus gehende Informationen über die Maschine und die Netzwerkkonfiguration
    - `ISAInfo2004_MachineName.log`
      Diese Log-Datei enthält ein Protokoll aller durchgeührten Aufgaben von `ISAInfo.js` sowie etwaige Fehlermeldungen.
- `ISAInfo.hta` ist ein Frontend, um die XML-Datei `ISAInfo2004_MachineName.xml` lesbar darzustellen. Ausserdem kann damit jede Export- oder Backup XML-Datei des ISA Server 2004 dargestellt werden!

Zu Support-, Dokumentations- und Vergleichszwecken füge ich hier ein Logfile an:

```
**************************************************************
ISAInfo 2004 version 1.0.RC2.1
Running on ISA2K4-002 as MSISAFAQ\Administrator
Started Sun Sep 5 20:29:15 UTC+0200 2004
**************************************************************

-- Exporting ISA configuration (this may take some time)...
-- Reading Array Logging configuration. -- Enumerating the servers in this array...
-- Reading additional ISA Server data...

-- Reading ISA signaled alerts...
-- Accessing WMI on ISA2K4-002
-- Executing WMI query 'select BuildNumber, BuildType, Caption, CSDVersion,
OSLanguage, OSProductSuite, SerialNumber, ServicePackMajorVersion,
ServicePackMinorVersion, SuiteMask, SystemDevice, SystemDirectory,
TotalVirtualMemorySize, Version, WindowsDirectory from Win32_OperatingSystem'

-- Executing WMI query 'select Compressed, FileSize, FSName, InitialSize, MaximumSize,
Name from Win32_PageFile'

-- Executing WMI query 'select Description, HotFixID from Win32_QuickFixEngineering
where HotFixID != 'File 1"

-- Executing WMI query 'select DisplayName, Description, Name, PathName, Started,
StartMode, StartName, State from Win32_SystemDriver'

-- Executing WMI query 'select DisplayName, Description, Name, PathName, ProcessId,
StartMode, StartName, State from Win32_Service'

-- Reading c:\boot.ini
-- Executing WMI query 'select BootupState, CurrentTimeZone, Description, Domain,
DomainRole, Manufacturer, Model, NumberOfProcessors, TotalPhysicalMemory from
Win32_ComputerSystem'

-- Executing WMI query 'select Availability, CapabilityDescriptions, Caption, Description,
DeviceID, InterfaceType, LastErrorCode, Manufacturer, Model, Name, Partitions, SCSIBus,
SCSILogicalUnit, SCSIPort, SCSITargetId, Size, Status from Win32_DiskDrive'

-- Executing WMI query 'select Caption, Description, DeviceID, DriveType, FileSystem,
```

FreeSpace, LastErrorCode, Size, VolumeDirty, VolumeName from Win32_LogicalDisk'

-- Executing WMI query 'select AdapterType, Availability, ConfigManagerErrorCode, Description, DeviceID, Index, LastErrorCode, Name, MACAddress, MaxNumberControlled, MaxSpeed, NetConnectionStatus, PowerManagementCapabilities, ServiceName, Speed, StatusInfo, TimeOfLastReset from Win32_NetworkAdapter'

-- Executing WMI query 'select Availability, CPUStatus, CurrentClockSpeed, DeviceID, l2CacheSize, l2CacheSpeed, Name from Win32_Processor'

-- Executing WMI query 'select AnswerMode, AttachedTo, Availability, Caption, ConfigurationDialog, Description, MaxBaudRateToPhone, MaxBaudRateToSerialPort, Model, ModemInfPath, Status from Win32_POTSModem'

-- Reading the event logs...
-- Executing WMI query 'select ComputerName, Data, EventCode, EventIdentifier, InsertionStrings, Message, SourceName, RecordNumber, TimeGenerated, TimeWritten, Type from Win32_NTLogEvent where LogFile = 'Application' and (EventType = '1' or EventType = '2' or EventType = '5') and TimeGenerated > '20040829203008.000000+120"

-- Executing WMI query 'select ComputerName, Data, EventCode, EventIdentifier, InsertionStrings, Message, SourceName, RecordNumber, TimeGenerated, TimeWritten, Type from Win32_NTLogEvent where LogFile = 'Security' and (EventType = '1' or EventType = '2' or EventType = '5') and TimeGenerated > '20040829203008.000000+120"

-- Executing WMI query 'select ComputerName, Data, EventCode, EventIdentifier, InsertionStrings, Message, SourceName, RecordNumber, TimeGenerated, TimeWritten, Type from Win32_NTLogEvent where LogFile = 'System' and (EventType = '1' or EventType = '2' or EventType = '5') and TimeGenerated > '20040829203008.000000+120"

-- Determining RemoteAccess service state...
-- Executing WMI query 'Select AllowMaximum, Caption, Description, MaximumAllowed, Name, Path, Status, Type From Win32_Share'

-- Executing WMI query 'select AccessMask, Compressed, Encrypted, FileSize, FileType, Manufacturer, Name from CIM_DataFile where Drive = 'C:' and Path = '\\Programme\\Microsoft ISA Server\\' and (FileType = 'Application' or FileType = 'Application Extension' or FileType = 'System File')'

-- Executing WMI query 'select AccessMask, Compressed, Encrypted, FileSize, FileType, Manufacturer, Name from CIM_DataFile where Drive = 'C:' and Path = '\\Programme\\Microsoft ISA Server\\clients\\' and (FileType = 'Application' or FileType = 'Application Extension' or FileType = 'System File')'

-- Executing WMI query 'select AccessMask, Compressed, Encrypted, FileSize, FileType, Manufacturer, Name from CIM_DataFile where Drive = 'C:' and Path = '\\Programme\\Microsoft ISA Server\\clients\\Program Files\\Microsoft Firewall Client 2004\\' and (FileType = 'Application' or FileType = 'Application Extension' or FileType = 'System File')'

-- Executing WMI query 'select AccessMask, Compressed, Encrypted, FileSize, FileType,

Manufacturer, Name from CIM_DataFile where Drive = 'C:' and Path = '\\Programme\\Microsoft ISA Server\\MSDE\\' and (FileType = 'Application' or FileType = 'Application Extension' or FileType = 'System File')'

-- Executing WMI query 'select AccessMask, Compressed, Encrypted, FileSize, FileType, Manufacturer, Name from CIM_DataFile where Drive = 'C:' and Path = '\\Programme\\Microsoft ISA Server\\Uninstall\\' and (FileType = 'Application' or FileType = 'Application Extension' or FileType = 'System File')'

-- Executing WMI query 'select AccessMask, Compressed, Encrypted, FileSize, FileType, Manufacturer, Name from CIM_DataFile where Drive = 'C:' and Path = '\\Programme\\Microsoft SQL Server\\MSSQL$MSFW\\Binn\\' and (FileType = 'Application' or FileType = 'Application Extension' or FileType = 'System File')'

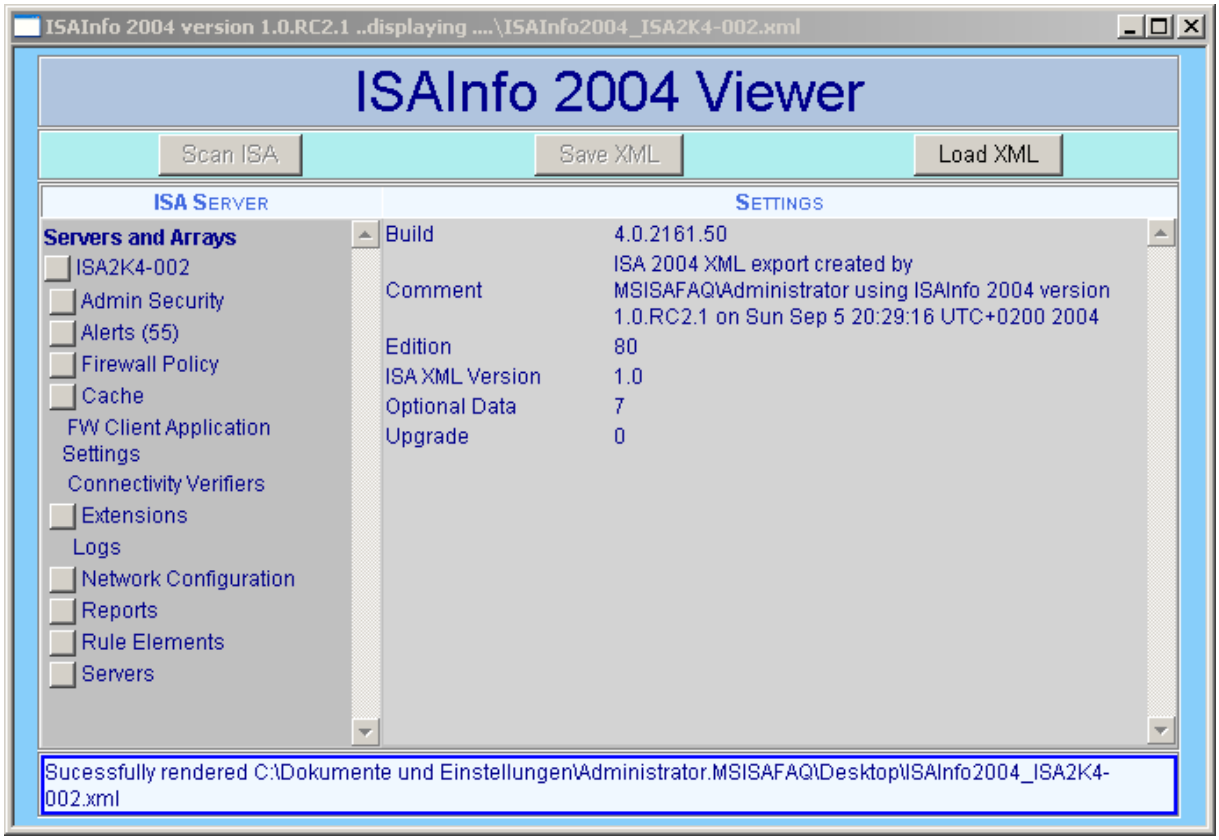
-- Reading registry tree at SOFTWARE\Microsoft\Microsoft SQL Server
-- Reading registry tree at SOFTWARE\Microsoft\MSSQLServer
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\bwcperf
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\ACECLIENT
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\BwcPerf
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\DNS intrusion detection filter
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\FTP Access Filter
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\ISA Server H.323 Filter
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\ISA Server RPC Filter
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\ISA Server Streaming Filter
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\Microsoft Firewall
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\Microsoft ISA Server Control
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\Microsoft ISA Server Job Scheduler
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\Microsoft ISA Server ReportGenerator
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\Microsoft ISA Server Storage
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\Microsoft ISA Server Web Proxy
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\Microsoft ISA Server WMS Proxy
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Eventlog\Application\POP Intrusion Detection Filter

-- Reading registry tree at
SYSTEM\CurrentControlSet\Services\Eventlog\Application\SmtpEvt
-- Reading registry tree at
SYSTEM\CurrentControlSet\Services\Eventlog\Application\SOCKS Filter
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Fweng
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\Fwsrv
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\H323Fltr
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\isactrl
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\isasched
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\isastg
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\MSSQL$MSFW
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\RemoteAccess
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\SocksFlt
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\tcpip
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\W3PCache
-- Reading registry tree at SYSTEM\CurrentControlSet\Services\W3Proxy
-- Accessing 'WScript.Shell'
-- Executing C:\WINDOWS\system32\cmd.exe /c IPCONFIG/ALL >> "C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt"
-- Reading C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt
-- Accessing 'WScript.Shell'
-- Executing C:\WINDOWS\system32\cmd.exe /c NETSTAT -R >> "C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt"
-- Reading C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt
-- Accessing 'WScript.Shell'
-- Executing C:\WINDOWS\system32\cmd.exe /c NETSH SHOW HELPER >>
"C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt"
-- Reading C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt
-- Accessing 'WScript.Shell'
-- Executing C:\WINDOWS\system32\cmd.exe /c WLBS DISPLAY >> "C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt"
-- Accessing 'WScript.Shell'
-- Executing C:\WINDOWS\system32\cmd.exe /c NETSTAT -ANO >> "C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt"
-- Reading C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_tempdata.txt
-- Accessing 'Msxml2.MXXMLWriter.3.0'
-- Accessing 'Msxml2.SAXXMLReader.3.0'
-- Cleaning up the XML...
-- Saving C:\Dokumente und
Einstellungen\Administrator.MSISAFAQ\Desktop\ISAInfo2004_ISA2K4-002.xml

ISAInfo 2004 version 1.0.RC2.1 completed at Sun Sep 5 20:31:03 UTC+0200 2004

Nachdem die Info-Datei erzeugt wurde kann das ISAInfo.hta-File ausgeführt werden. Es wird folgende Oberfläche gestartet:

Über den Button "Load XML" kann die anzusehende XML-Datei ausgewählt und geöffnet werden.



Über das Menü auf der linken Seite kann durch die Konfiguration gegangen werden. Z.B. lassen sich die konfigurierten Firewallrichtlinien anzeigen:

Hinweis: ISAInfo.hta kann auch auf einem anderen Rechner ausgeführt werden, um dort die ISA Konfiguration zu betrachten.

Schönheitskorrektur: SQL Server-Dienst Manager

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

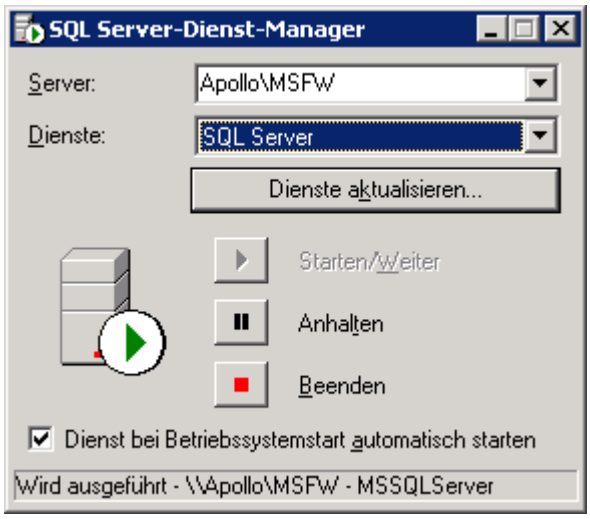
Der vorliegende Artikel beschreibt die Beseitigung eines kleinen Schönheitsfehlers im Zusammenhang mit der durch den ISA Server 2004 installierten MSDE Datenbank.

Standardmäßig kann man im Systemtray keinen Status der Datenbank einsehen:

Der Status der Datenbank ist nicht ersichtlich. Dies kann jedoch ganz einfach geändert werden:

Öffnen des SQL Server-Dienst Manager (durch Doppelklick):

Im Feld "Server" den Namen des ISA Server Computers und die zugehörige SQL-Instanz angegeben:



Anschließend kann man durch "Dienste aktualisieren" den SQL Serverdienst auswählen und das Fenster schließen.

Künftig erscheint das Trayicon mit der Statusinformation:

Erstellen einer Firewallrichtlinie am Beispiel von POP3

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Im Artikel Firewallrichtlinien wurde beschrieben, was Firewallrichtlinien sind und wie sie funktionieren. In dem vorliegenden Artikel wird die Erstellung einer solchen Richtlinie anhand einer Beispielkonfiguration beschrieben und gezeigt.

Ausgangssituation: Benutzerin Birgit soll während der Arbeitszeit (09:00-12:00 und 13:00-17:00 Uhr) und auch während der Mittagspause (12:00-13:00 Uhr) mit ihrem Outlook von ihrem fest zugewiesenen Arbeitsplatzrechner von einen im Internet stehenden Mailserver per POP3 Mails abholen können.

Erinnern wir uns an die Leitregel für die Firewallrichtlinien:

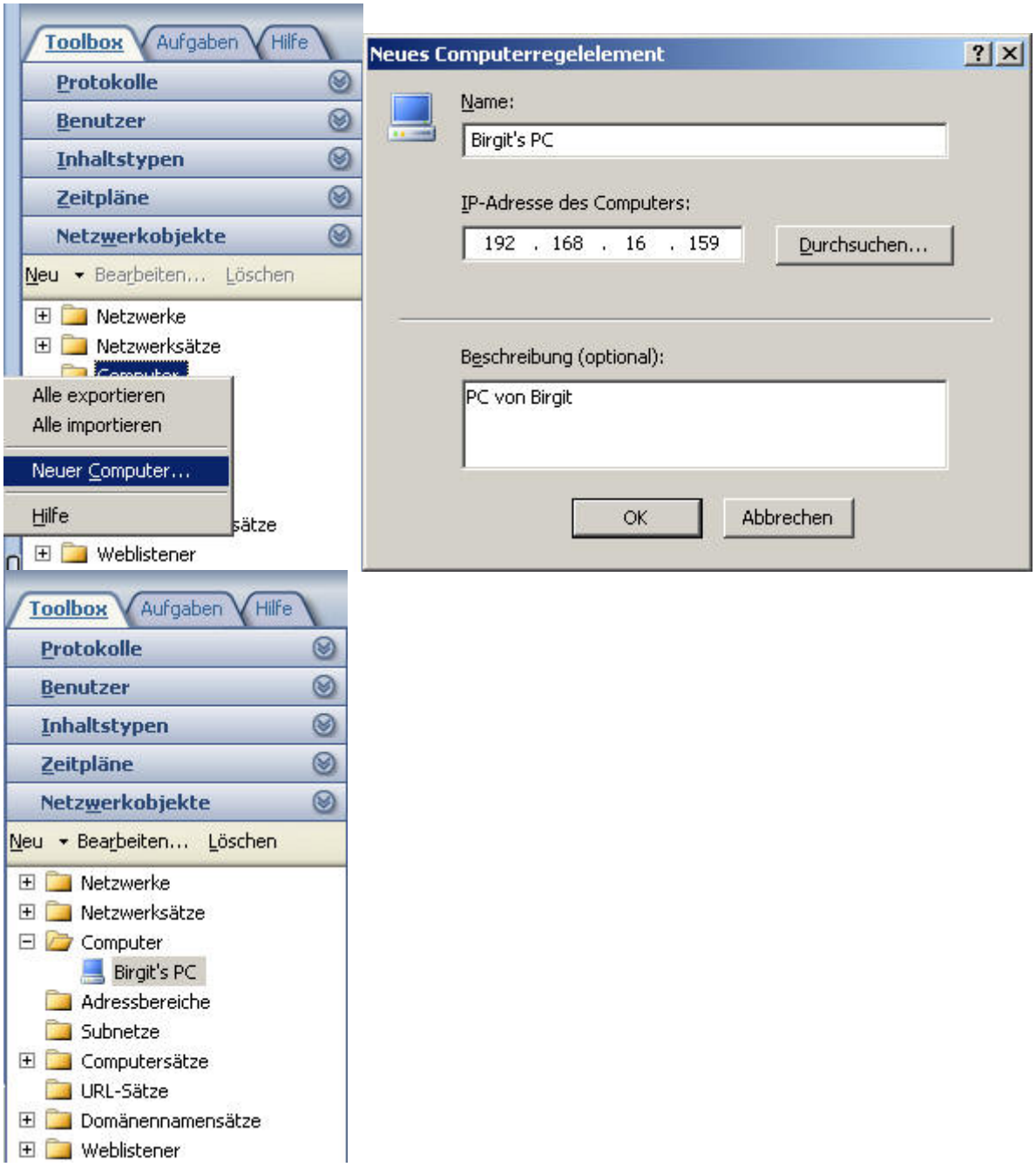
Aktion für Verkehr von Benutzer aus Quelle zu Ziel mit Einschränkungen

In diesem Beispiel gilt:

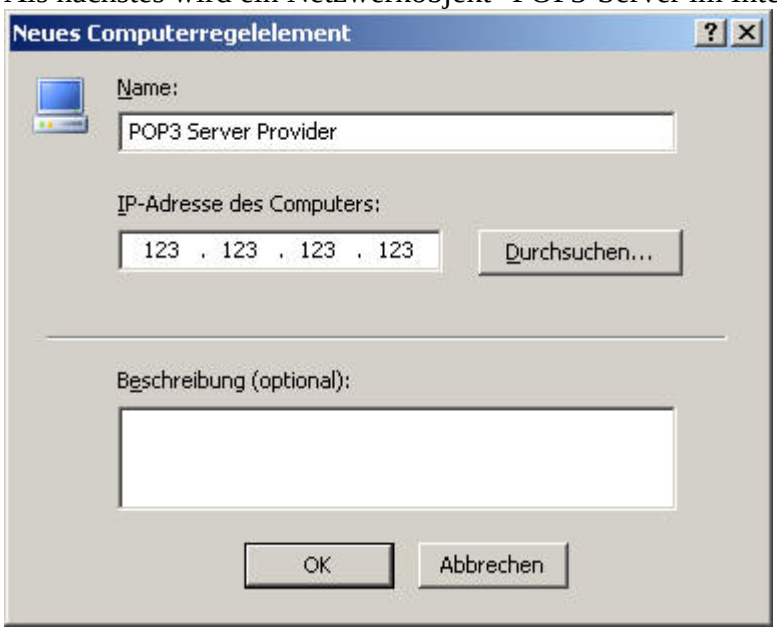
- Aktion: zulassen
- Verkehr: POP3
- Benutzer: Birgit
- Quelle: Birgit's Computer
- Ziel: POP3 Server des Providers
- Einschränkungen: Arbeitszeit und Mittagspause

Mit der Toolbox sollten wir uns zuerst Elemente für "Birgit's Computer", "POP3 Server des Providers", "Arbeitszeit" und "Mittagspause" erstellen. Sofern auf Birgit's Computer der Firewallclient ausgeführt wird, könnte zusätzlich zur Einschränkung von ihrem PC auch ihre Benutzerauthentifizierung erzwungen werden, die bei nicht-HTTP/FTP-Verkehr ausschließlich mittels des Firewallclients möglich ist.

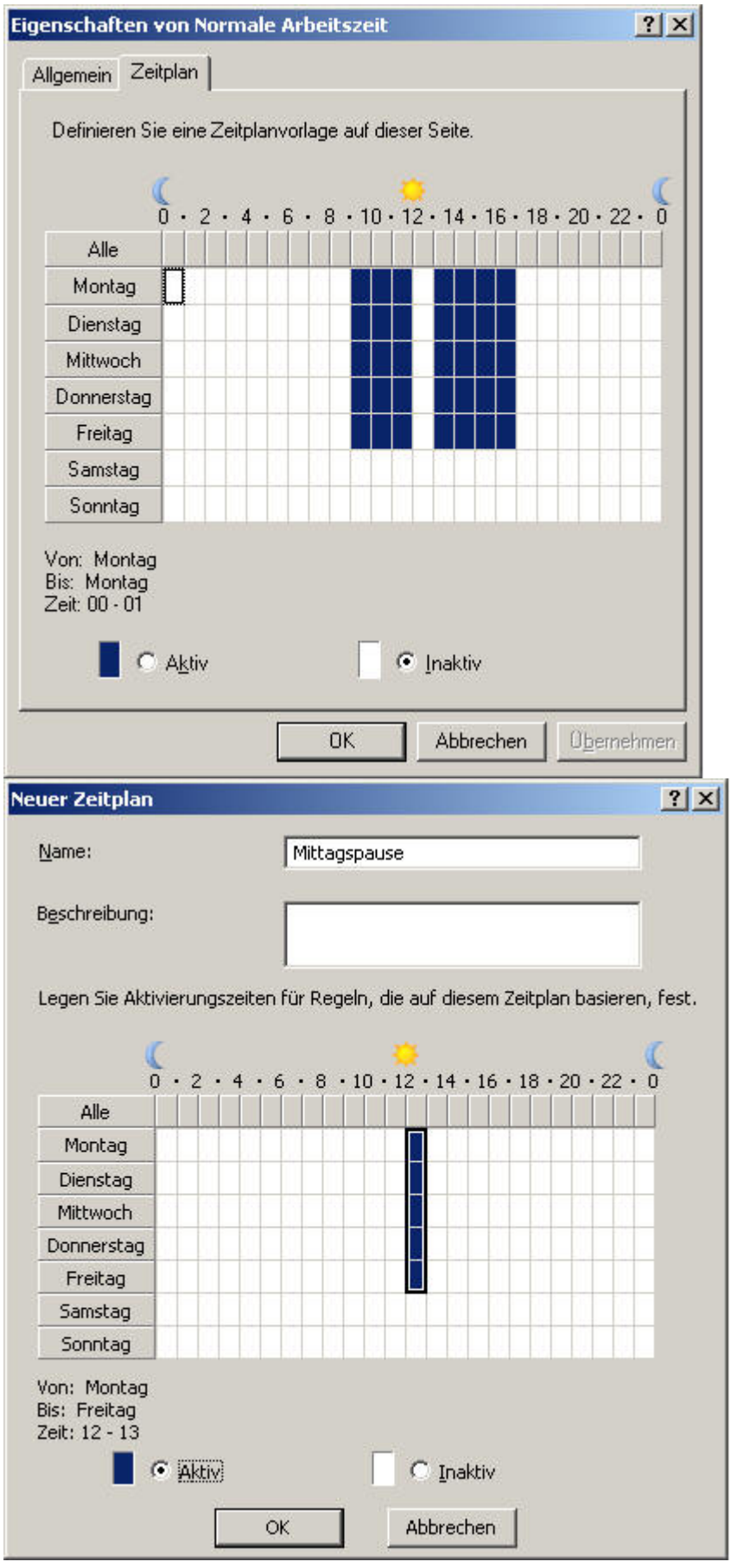
Zuerst wird ein neues Netzwerkobjekt "Birgit's PC" erstellt, welches anhand seiner IP Adresse charakterisiert wird:


Toolbox
Aufgaben
Hilfe
Protokolle
Benutzer
Inhaltstypen
Zeitpläne
Netzwerkobjekte
Neu
Bearbeiten...
Löschen
Netzwerke
Netzwerksätze
Alle exportieren
Alle importieren
Neuer Computer...
Hilfe
Weblistener
Neues Computerregelelement
Name:
Birgit's PC
IP-Adresse des Computers:
192 . 168 . 16 . 159
Durchsuchen...
Beschreibung (optional):
PC von Birgit
OK
Abbrechen
Computer
Birgit's PC
Adressbereiche
Subnetze
Computersätze
URL-Sätze
Domänennamensätze

Als nächstes wird ein Netzwerkobjekt "POP3-Server im Internet" erstellt:



Nun noch schnell die beiden Zeitpläne anpassen bzw. erstellen:

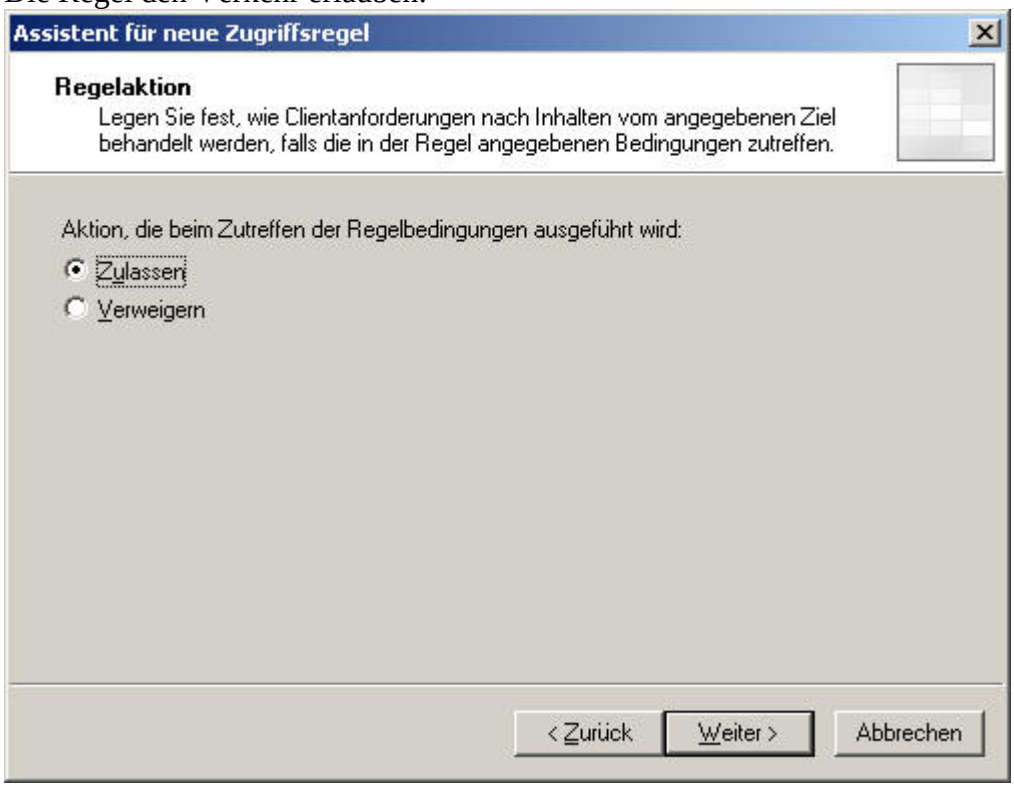


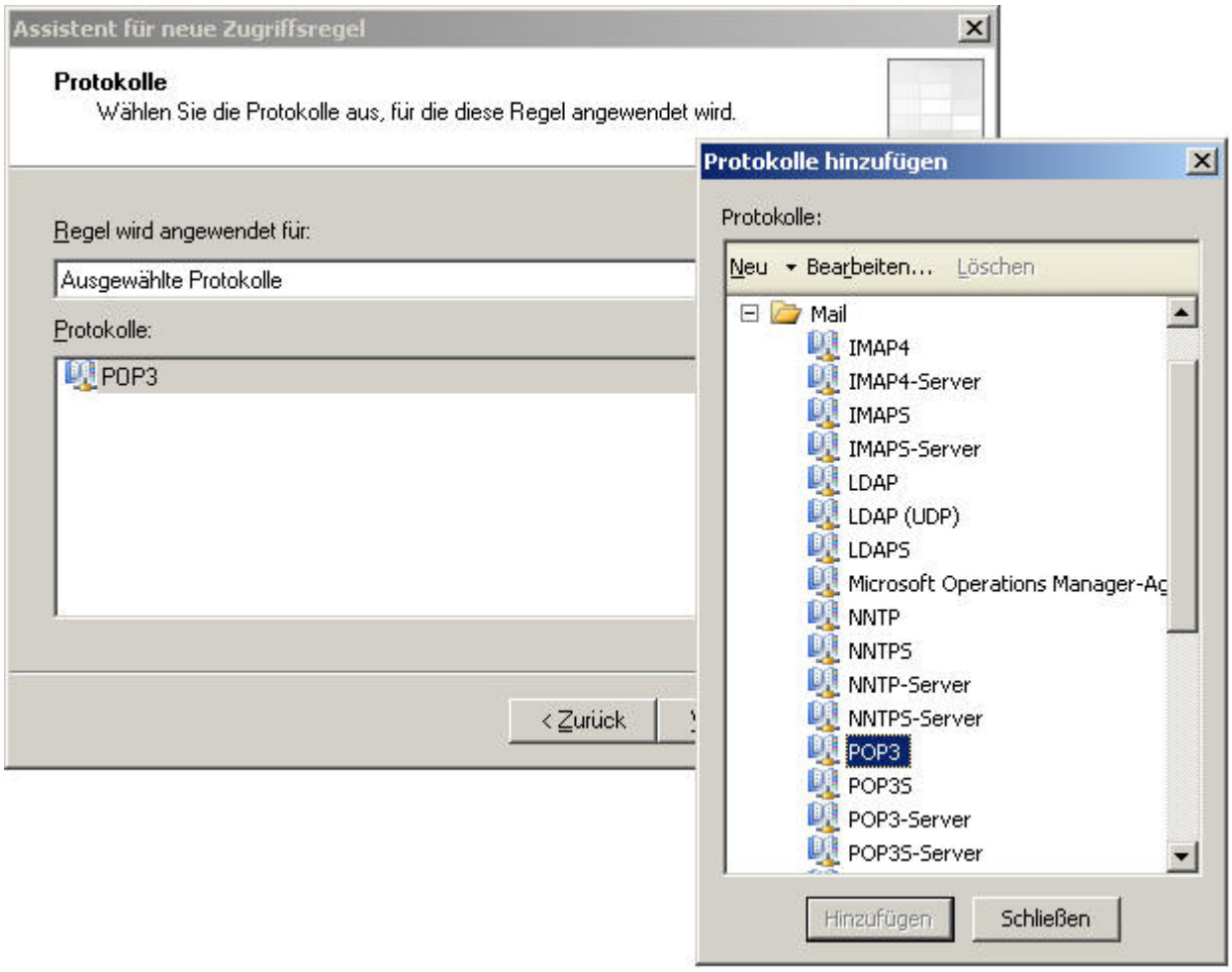
Nun haben wir alle Bauelemente zusammen und können die Firewallrichtlinie erstellen:

Dazu aus dem Aufgabenbereich den Punkt "Neue Zugriffsregel erstellen" auswählen.

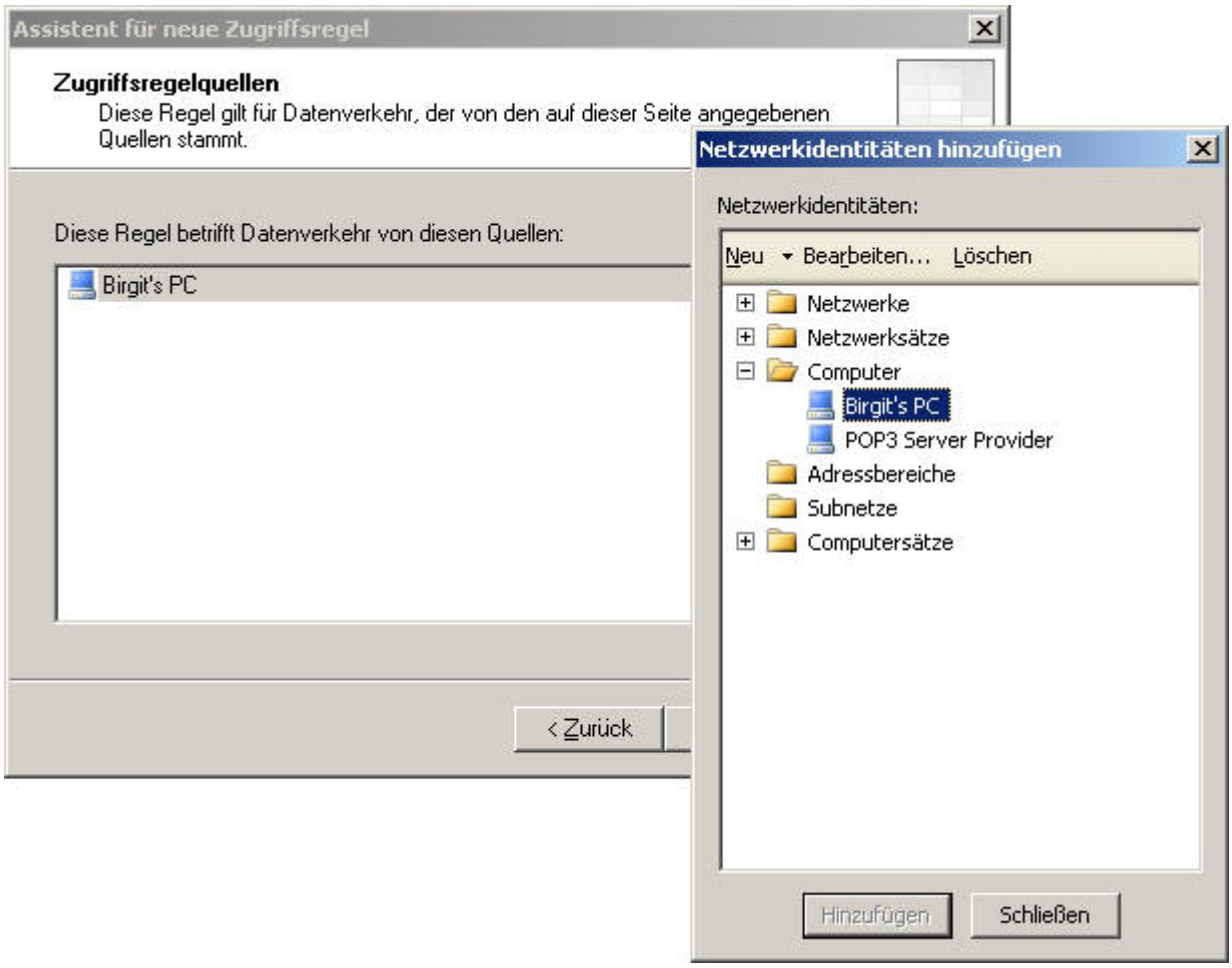
Für die Zugriffsregel sollte ein eindeutiger Name verwendet werden. Das erleichtert später die Übersicht.

Die Regel den Verkehr erlauben:



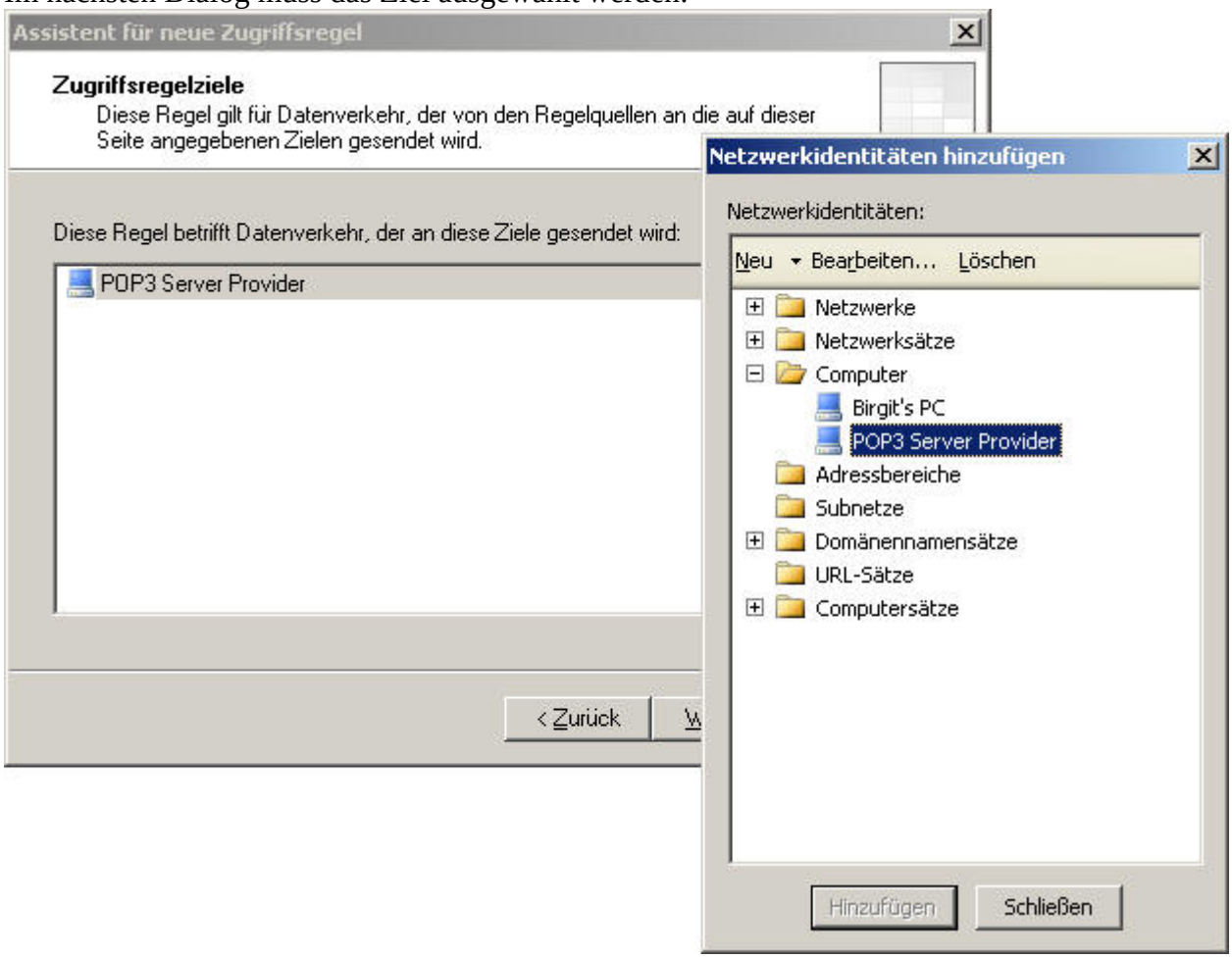


Durch Doppelklick auf das POP3-Element in der Toolbox wird es dem Assistenten hinzugefügt.



Als nächstes wird das Quellobjekt angegeben.

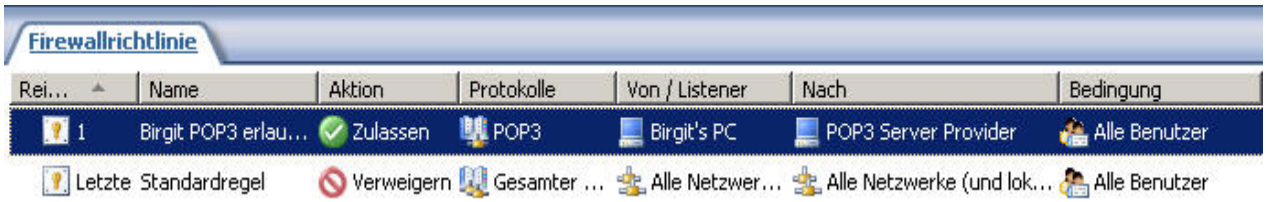
Im nächsten Dialog muss das Ziel ausgewählt werden:



Die letzte Auswahlbox kann übernommen werden. Hier könnte, wie bereits erwähnt, zusammen mit dem Firewallclient eine Authentifizierung auf Benutzerebene für diese Zugriffsrichtlinie erzwungen werden. Damit könnte Paul keinen Zugriff auf POP3 bekommen, wenn er an Birgit's Rechner sitzt, was in unserem Beispiel ohne Firewallclient möglich ist.

Zum Schluss gibt es eine Zusammenfassung - die ggfs. für Dokumentationszwecke (hier funktioniert drag-and-drop) weiterverwendet werden kann:

Nun ist die neue Richtlinie erstellt:



Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

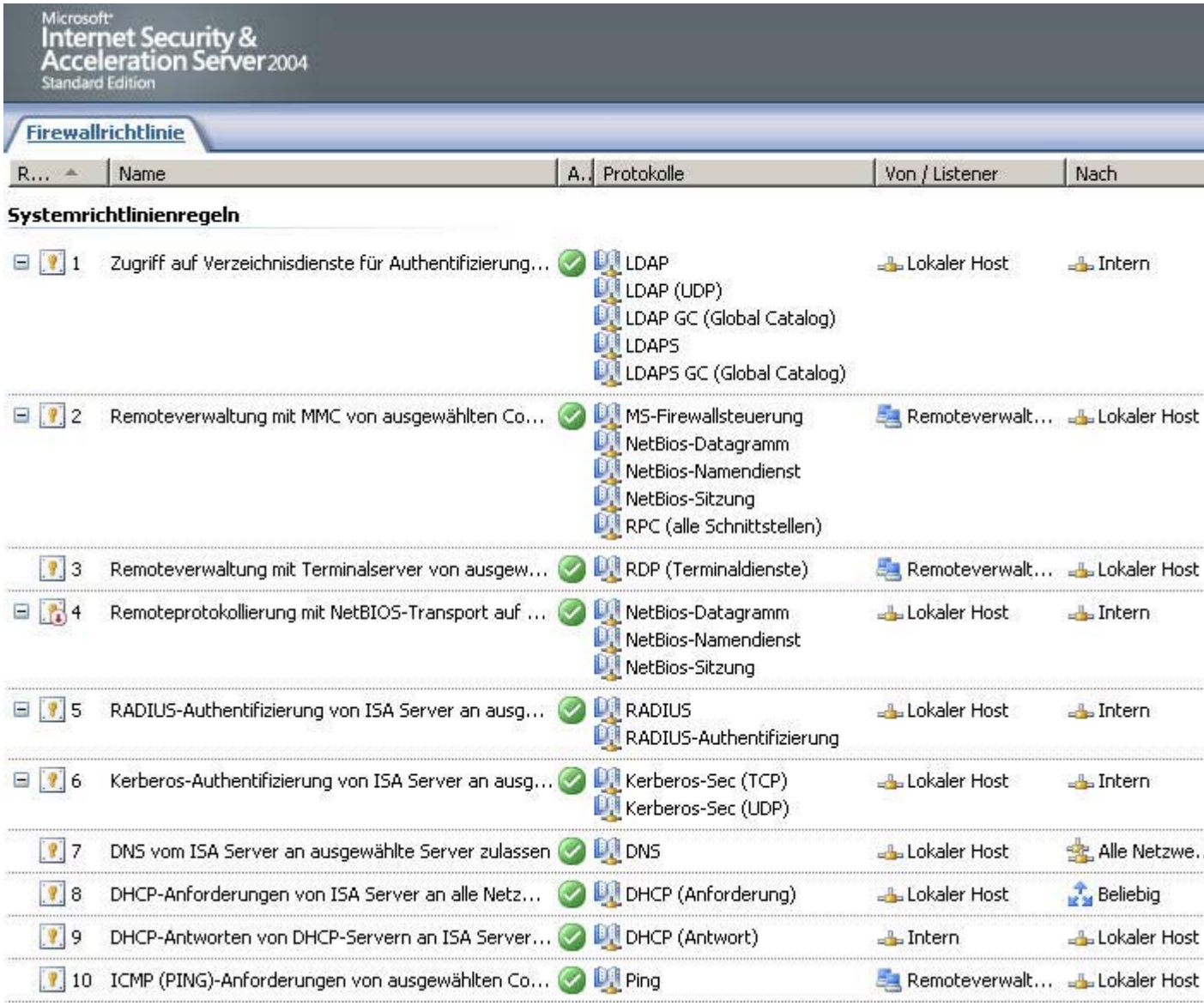
Systemrichtlinien: Firewallrichtlinien für den ISA Server selber

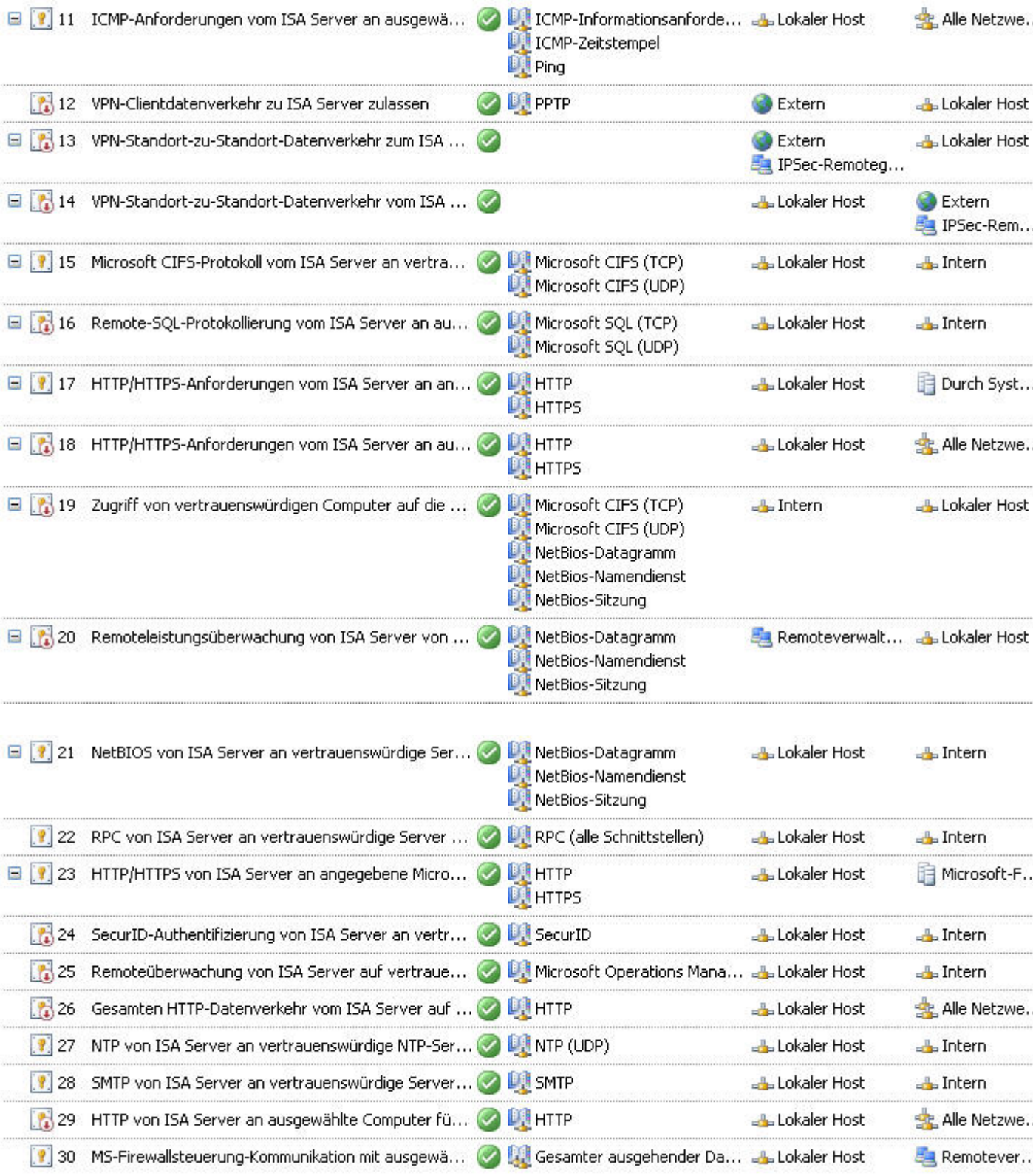
---

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Im Artikel Firewallrichtlinien wurde beschrieben, wozu Firewallrichtlinien benötigt werden und wie sie funktionieren. Dort wurde auch erwähnt, dass es neben den individuellen Firewallrichtlinien weitere Richtlinien gibt. Der ISA Server selber benötigt für seine Funktionalität eigene Richtlinien, die so genannten Systemrichtlinien. In ihnen wird festgelegt, welche Protokolle bzw. Verbindungen wohin der ISA Server selber nutzen darf. Nach der Installation sind insgesamt 30 vordefinierte Systemrichtlinien vorhanden, jedoch sind nicht alle aktiviert:


Microsoft
Internet Security & Acceleration Server 2004
Standard Edition
Firewallrichtlinie
R...
Name
A..
Protokolle
Von / Listener
Nach
Systemrichtlinienregeln
1 Zugriff auf Verzeichnisdienste für Authentifizierung... LDAP, LDAP (UDP), LDAP GC (Global Catalog), LDAPS, LDAPS GC (Global Catalog) Lokaler Host Intern
2 Remoteverwaltung mit MMC von ausgewählten Co... MS-Firewallsteuerung, NetBios-Datagramm, NetBios-Namendienst, NetBios-Sitzung, RPC (alle Schnittstellen) Remoteverwalt... Lokaler Host
3 Remoteverwaltung mit Terminalserver von ausgew... RDP (Terminaldienste) Remoteverwalt... Lokaler Host
4 Remoteprotokollierung mit NetBIOS-Transport auf ... NetBios-Datagramm, NetBios-Namendienst, NetBios-Sitzung Lokaler Host Intern
5 RADIUS-Authentifizierung von ISA Server an ausg... RADIUS, RADIUS-Authentifizierung Lokaler Host Intern
6 Kerberos-Authentifizierung von ISA Server an ausg... Kerberos-Sec (TCP), Kerberos-Sec (UDP) Lokaler Host Intern
7 DNS vom ISA Server an ausgewählte Server zulassen DNS Lokaler Host Alle Netzwe..
8 DHCP-Anforderungen von ISA Server an alle Netz... DHCP (Anforderung) Lokaler Host Beliebig
9 DHCP-Antworten von DHCP-Servern an ISA Server... DHCP (Antwort) Intern Lokaler Host
10 ICMP (PING)-Anforderungen von ausgewählten Co... Ping Remoteverwalt... Lokaler Host

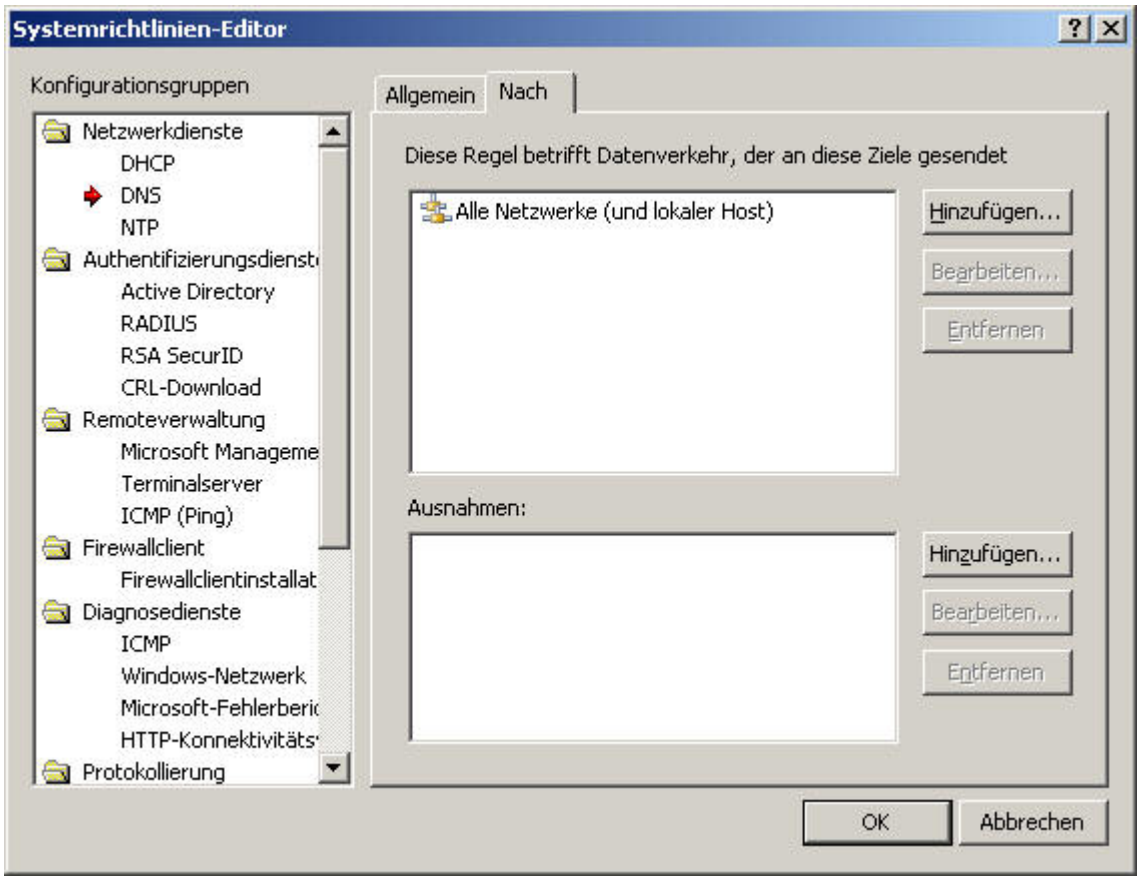


11	ICMP-Anforderungen vom ISA Server an ausgewä...	ICMP-Informationsanforde... ICMP-Zeitstempel Ping	Lokaler Host	Alle Netzwe...
12	VPN-Clientdatenverkehr zu ISA Server zulassen	PPTP	Extern	Lokaler Host
13	VPN-Standort-zu-Standort-Datenverkehr zum ISA ...		Extern IPSec-Remoteg...	Lokaler Host
14	VPN-Standort-zu-Standort-Datenverkehr vom ISA ...		Lokaler Host	Extern IPSec-Rem...
15	Microsoft CIFS-Protokoll vom ISA Server an vertra...	Microsoft CIFS (TCP) Microsoft CIFS (UDP)	Lokaler Host	Intern
16	Remote-SQL-Protokollierung vom ISA Server an au...	Microsoft SQL (TCP) Microsoft SQL (UDP)	Lokaler Host	Intern
17	HTTP/HTTPS-Anforderungen vom ISA Server an an...	HTTP HTTPS	Lokaler Host	Durch Syst...
18	HTTP/HTTPS-Anforderungen vom ISA Server an au...	HTTP HTTPS	Lokaler Host	Alle Netzwe...
19	Zugriff von vertrauenswürdigen Computer auf die ...	Microsoft CIFS (TCP) Microsoft CIFS (UDP) NetBios-Datagramm NetBios-Namendienst NetBios-Sitzung	Intern	Lokaler Host
20	Remoteleistungsüberwachung von ISA Server von ...	NetBios-Datagramm NetBios-Namendienst NetBios-Sitzung	Remoteverwalt...	Lokaler Host
21	NetBIOS von ISA Server an vertrauenswürdige Ser...	NetBios-Datagramm NetBios-Namendienst NetBios-Sitzung	Lokaler Host	Intern
22	RPC von ISA Server an vertrauenswürdige Server ...	RPC (alle Schnittstellen)	Lokaler Host	Intern
23	HTTP/HTTPS von ISA Server an angegebene Micro...	HTTP HTTPS	Lokaler Host	Microsoft-F...
24	SecurID-Authentifizierung von ISA Server an vertr...	SecurID	Lokaler Host	Intern
25	Remoteüberwachung von ISA Server auf vertraue...	Microsoft Operations Mana...	Lokaler Host	Intern
26	Gesamten HTTP-Datenverkehr vom ISA Server auf ...	HTTP	Lokaler Host	Alle Netzwe...
27	NTP von ISA Server an vertrauenswürdige NTP-Ser...	NTP (UDP)	Lokaler Host	Intern
28	SMTP von ISA Server an vertrauenswürdige Server...	SMTP	Lokaler Host	Intern
29	HTTP von ISA Server an ausgewählte Computer fü...	HTTP	Lokaler Host	Alle Netzwe...
30	MS-Firewallsteuerung-Kommunikation mit ausgewä...	Gesamter ausgehender Da...	Lokaler Host	Remotever...

Hinweis: Unten gibt es weiterführenden Erklärungen.

Es gibt 2 Möglichkeiten, die Systemrichtlinien zu bearbeiten:

Mittels dieses Weges erhalten Sie ein neues vorgelagertes Fenster mit den Systemrichtlinien:



Hiermit können die Systemrichtlinien einfach verwaltet werden.

Wer lieber die Ansicht wie sie auch bei den Firewallrichtlinien verwendet wird bevorzugt kann sich im Aufgabenbereich der Firewallrichtlinien die Systemrichtlinien einblenden lassen und gelangt somit zu Übersicht, wie sie zu Beginn dieses Artikels verwendet wird:

Die folgende Tabelle soll helfen, die Funktionsweise und den Zweck jeder Systemrichtlinie zu verstehen:

nach oben

1		Authentifizierungsdienste: Zugriff auf Verzeichnisdienste für Authentifizierungszwecke zulassen	Gestattet dem ISA Server Zugriff auf das Active Directory des als intern (und somit vertrauenswürdig) definierten Netzwerk.
2		Remoteverwaltung: Remoteverwaltung mit MMC von ausgewählten Computern zulassen	Gewährt allen Computern des Computersets "Remoteverwaltungscomputer" den Remotezugriff auf die ISA Konfiguration mittels der MMC.
3		Remoteverwaltung: Remoteverwaltung mit Terminalserver von ausgewählten Computern zulassen	Gewährt allen Computern des Computersets "Remoteverwaltungscomputer" den Remotezugriff auf die ISA Konfiguration mittels Remotedesktop.
4		Remoteverwaltung: Remoteprotokollierung auf vertrauenswürdigen Servern mit NetBIOS zulassen	Der ISA Server darf NetBIOS Anfragen/Verbindungen zu allen internen Rechnern aufbauen.
5		Authentifizierungsdienste: RADIUS-Authentifizierung von ISA Server an vertrauenswürdige RADIUS-Server zulassen	Gestattet dem ISA Server Zugriff auf einen RADIUS/IAS Server im internen Netzwerk zur Authentifizierung.

6		Authentifizierungsdienste: Kerberos-Authentifizierung von ISA Server an vertrauenswürdige Server zulassen	Gestattet dem ISA Server eine Kerberos-Authentifizierung gegen Server im internen Netzwerk zur Authentifizierung.
7		Netzwerkdienste: DNS vom ISA Server an ausgewählte Server zulassen	Erlaubt dem ISA Server, DNS-Anfragen zwecks Namensauflösung in alle Netzwerke zu stellen und die Antwort zu empfangen.
8		Netzwerkdienste: DHCP-Anforderungen von ISA Server an alle Netzwerke zulassen	Erlaubt dem ISA Server selber, eine oder mehrer IP-Adressen per DHCP zu beziehen.
9		Netzwerkdienste: DHCP-Antworten von DHCP-Servern an ISA Server zulassen	Erlaubt Clients des internen Netzwerkes DHCP Anfragen an den ISA Server zu senden und eine Antwort zu empfangen.
10		Netzwerkdienste: ICMP (PING)-Anforderungen von ausgewählten Computern an ISA Server zulassen	Erlaubt allen Computern des Computersets "Remoteverwaltungscomputer" eine ping-Anforderung an den ISA Server zu stellen.
11		Diagnosedienste: ICMP-Anforderungen vom ISA Server an ausgewählte Server zulassen	Gestattet dem ISA Server eine ping-Anforderung in alle Netzwerke zu senden.
12		VPN: VPN-Clientdatenverkehr auf ISA Server zulassen. VPN-Systemrichtlinienregeln basieren auf VPN-Eigenschaften und auf dem VPN-Koten in der ISA Server-Verwaltung konfiguriert.	Erlaubt Clients aus dem externen Netz eine PPTP-VPN-Verbindung zum ISA Server herzustellen.
13		VPN: VPN-Standort-zu-Standort-Datenverkehr zum ISA Server zulassen. VPN-Systemrichtlinienregeln basieren auf VPN-Eigenschaften, die im VPN-Knoten der ISA Server-Verwaltung konfiguriert werden.	Richtlinie, die für eine Remotestandortanbindung notwendig ist. Sie erlaubt den Verkehr vom Remotestandort zum ISA Server.
14		VPN: VPN-Standort-zu-Standort-Datenverkehr vom ISA Server zulassen. VPN-Systemrichtlinienregeln basieren auf VPN-Eigenschaften, die im VPN-Knoten der ISA Server-Verwaltung konfiguriert werden.	Richtlinie, die für eine Remotestandortanbindung notwendig ist. Sie erlaubt den Verkehr vom ISA Server zum Remotestandort.
15		Authentifizierungsdienste: Microsoft CIFS von ISA Server auf vertrauenswürdige Server zulassen	Erlaubt dem ISA Server, einen Filesystemzugriff auf interne Rechner.
16		Protokollierung: Remote-SQL-Protokollierung vom ISA Server an ausgewählte Server zulassen	Erlaubt dem ISA Server die Kommunikation mit einem internen SQL-Server zwecks Protokollierung.
17		Verschiedene: HTTP/HTTPS-Anforderungen von ISA Server an angegebene Sites zulassen	Erlaubt dem ISA Server den Zugriff via HTTP und HTTPS auf die Seiten *.microsoft.com;

			*.windows.com und *.windowsupdate.com
18		Netzwerkdienste: HTTP/HTTPS-Anforderungen vom ISA Server an ausgewählte Server für Konnektivitätsverifizierungen zulassen	Erlaubt bei konfigurierter Konnektivitätsverifizierung dem ISA Server, Webseiten aus allen Netzwerken herunterzuladen.
19		Firewallclient: Zugriff von vertrauenswürdigen Computer auf die Firewallclient-Installationsfreigabe auf dem ISA Server zulassen	Wird benötigt, wenn der Firewallclientinstallationsordner auf dem ISA Server als Freigabe vorhanden ist. Damit können interne Clients darauf zugreifen.
20		Remoteüberwachung: Remoteleistungsüberwachung von ISA Server von vertrauenswürdigen Servern zulassen	Erlaubt allen Computern des Computersets "Remoteverwaltungscomputer" NetBIOS Sitzungen zum ISA Server zwecks Leistungsüberwachung herzustellen.
21		Diagnosedienste: NetBIOS von ISA Server auf vertrauenswürdige Server zulassen	Der ISA Server darf NetBIOS Anfragen/Verbindungen zu allen internen Rechnern aufbauen.
22		Authentifizierungsdienste: RPC von ISA Server auf vertrauenswürdige Server zulassen	ISA Server erlauben, RPC-Verbindungen zum internen Netzwerk aufzubauen.
23		Diagnosedienste: HTTP/HTTPS von ISA Server an angegebene Microsoft-Fehlerberichterstattungs-Sites zulassen	Erlaubt der Fehlerberichtsfunktion den Zugriff auf die Microsoft-Fehlerberichtsseite *.watson.microsoft.com
24		Authentifizierungsdienste: SecurID-Authentifizierung von ISA Server an ausgewählte Server zulassen	Wird benötigt, wenn der SecurID-Filter aktiv ist für Authentifizierungsanfragen zu internen SecurID-Servern.
25		Remoteüberwachung: Remoteüberwachung von ISA Server auf vertrauenswürdigen Servern mithilfe des Microsoft Operations Manager-Agents zulassen.	Wird benötigt, wenn ein MOM-Server den ISA Server überwachen soll.
26		Authentifizierungsdienste: HTTP von ISA Server an ausgewählte Netzwerke für das Downloaden aktualisierten Zertifikatsperrlisten zulassen	Erlaubt dem ISA Server, die neusten Zertifikatsperrlisen via HTTP von allen Netzwerken abzurufen.
27		Netzwerkdienste: NTP von ISA Server an vertrauenswürdige NTP-Server zulassen	Gestattet dem ISA Server eine Zeitsynchronisation durchzuführen.
28		Remoteüberwachung: SMTP von ISA Server an vertrauenswürdige Server zulassen	Erlaubt dem ISA Server z.B. für Alarmbenachrichtigungen Mails per SMTP an das interne

			Netzwerk zu senden.
29		Verschiedenes: HTTP von ISA Server an ausgewählte Computer für Inhaltdownloadaufträge zulassen	Wenn geplante Inhaltsdownload-Aufträge existieren, erlaubt diese dann aktivierte Richtlinie den HTTP-Verkehr.
30		Remoteverwaltung: Remoteverwaltungscomputern gestatten, auf dem ISA Server-Computer ausgeführte Dienste zu verwalten.	Erlaubt sämtlichen Verkehr vom ISA Server zu allen Computern des Computersets "Remoteverwaltungscomputer"

nach oben

Systemrichtlinien können nicht gelöscht werden. Es können auch keine Weiteren erstellt werden. Sie können jedoch Systemrichtlinien deaktivieren oder in begrenztem Umfang anpassen. Um den Umfang zu erweitern sollten Sie eine zusätzliche Firewallrichtlinie erstellen, was anhand des Beispiels Ping erläutert wird.

Sie sollten diese Systemrichtlinien in das Firewallkonzept mit einbeziehen und an die individuellen Bedürfnisse anpassen.

Ein- und Ausgehende ping-Anfragen konfigurieren

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Im Artikel Systemrichtlinien wurden zwei Systemrichtlinien (Nr. 10 und 11) vorgestellt, die bestimmte ICMP Verbindungen von und zum ISA Server zulassen. Diese ICMP Verbindungen (ICMP-Code 0, ICMP-Typ 8) werden durch das Kommandozeilentool ping verwendet um die Erreichbarkeit entfernter Computer zu überprüfen.

Im Auslieferungszustand sind folgende ping-Anfragen zugelassen:

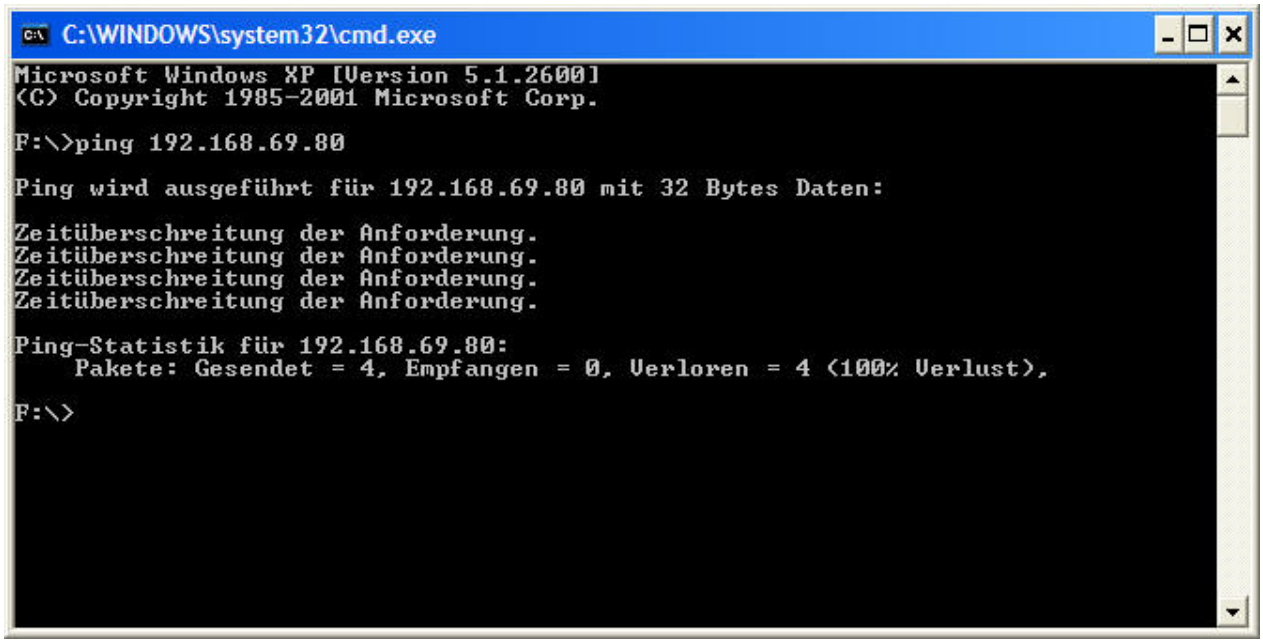
- Von Computern des Computersatzes "Remoteverwaltungscomputer" zum ISA Server
- Vom ISA Server in alle Netzwerke

Diese beiden Richtlinien sollten im Normalfall zu Diagnosezwecken ausreichend sein. In den allermeisten Fällen besteht keinerlei Notwendigkeit, dass der ISA Server aus anderen Netzen oder von anderen Clients aus per ping erreichbar ist. Aus Sicherheitsgründen sollten Änderungen am Regelwerk diesbezüglich gut überlegt werden und nur bei wichtigen Gründen durchgeführt werden.

Der hier vorliegende Artikel stellt die zusätzlichen Konfigurationsschritte dar, um den ISA Server von extern anzupingen und um internen Clients zu erlauben, externe Rechner anzupingen.

1. Konfiguration des ISA Server für eingehende ping-Anfragen

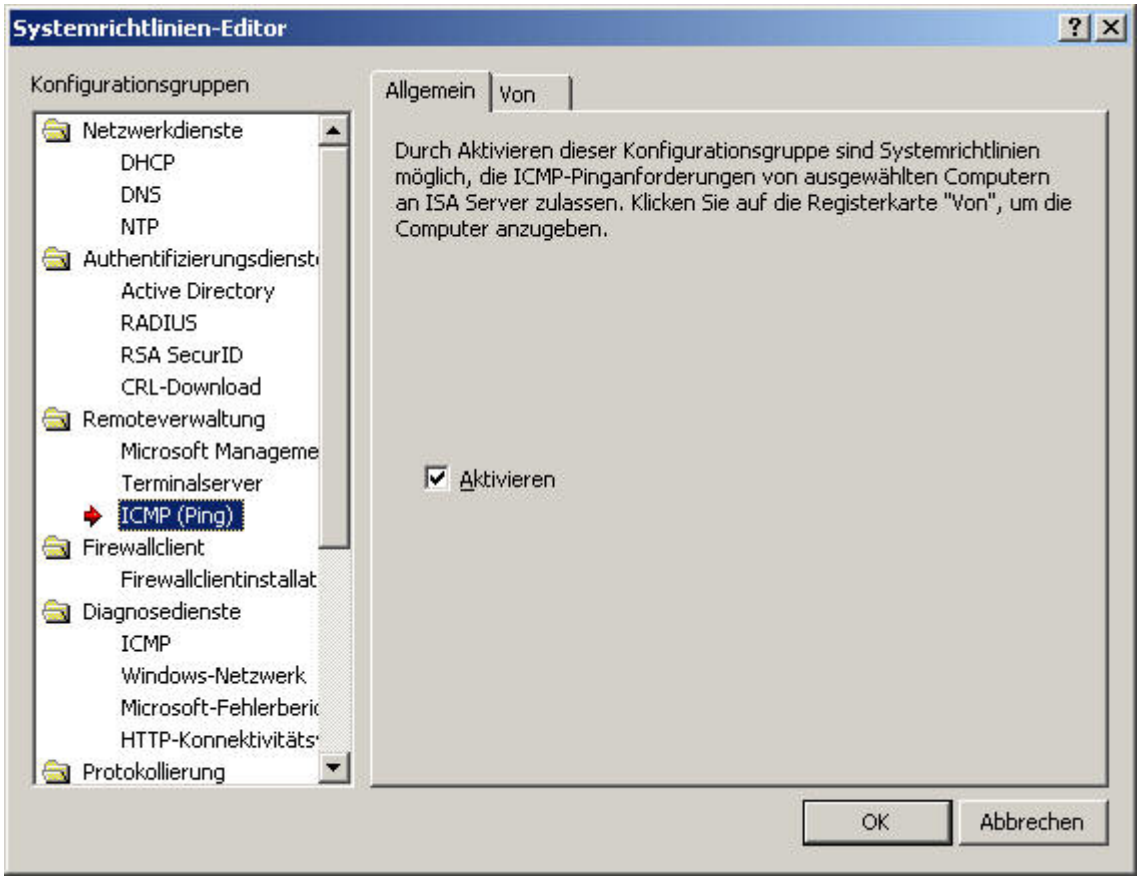
Wie bereits erwähnt, reagiert der ISA Server nicht auf ping-Anfragen externer Clients:



Es gibt prinzipiell zwei Wege, diese Konfigurationserweiterung vorzunehmen. Man kann sowohl die bestehende Default-Systemrichtlinie verändern oder eine neue Firewallrichtlinie erstellen. Beide Wege werden hier beschrieben. Welcher Weg sinnvoller ist, kann nicht pauschal beantwortet werden.

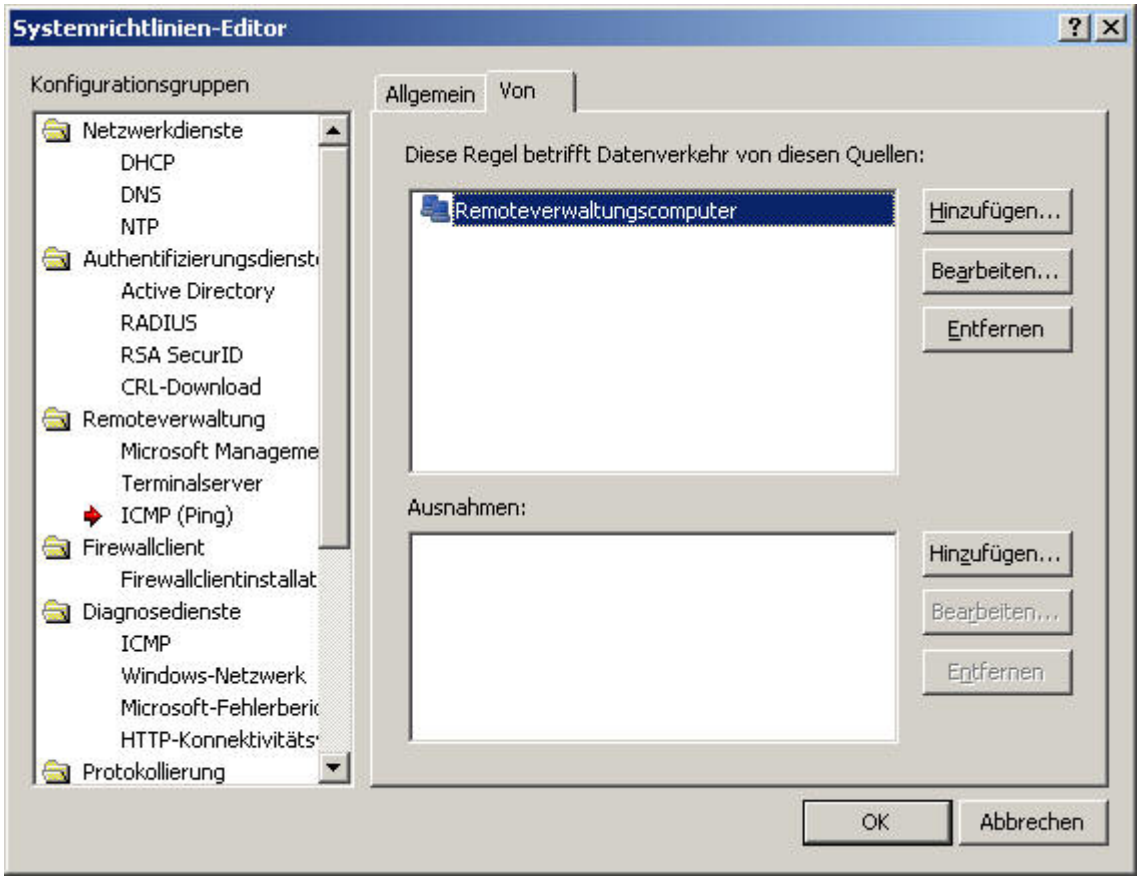
1a) Änderung der Systemrichtlinie

Öffnen Sie den Systemrichtlinien-Editor über das Kontextmenü des Management-Konsole-Knoten "Firewallrichtlinie" und zeigen Sie auf den Punkt Remoteverwaltung - ICMP (Ping):

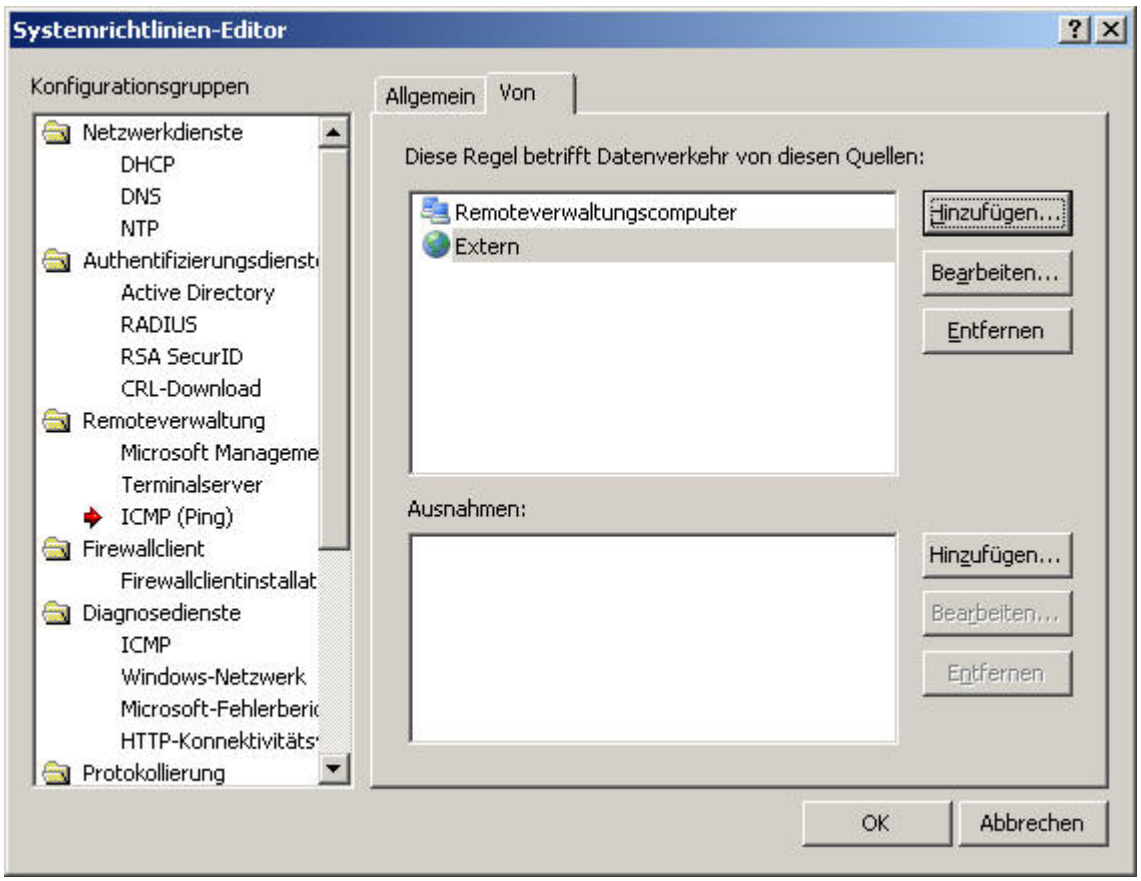


Wie bereits erwähnt, ist diese Richtlinie aktiv. Hier könnte sie auch deaktiviert werden. Dann kann der ISA Server nicht mehr angepingt werden.

Im folgenden Screenshot sehen Sie die Standardeinstellung:



Fügen Sie über den "Hinzufügen..."-Button z.B. das Externe Netzwerk hinzu. Natürlich können Sie hier je nach Firewallkonzept auch nur bestimmte Objekte hinzufügen.

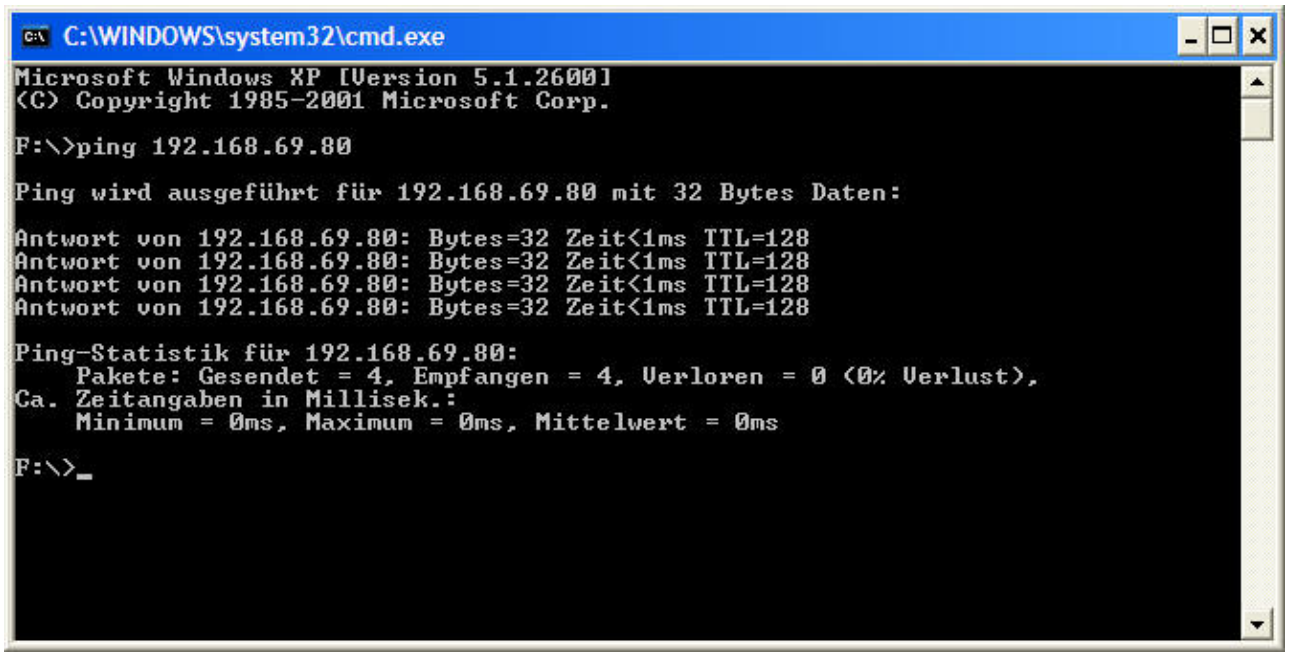


Beenden Sie den Systemrichtlinien-Editor mit OK.

Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

Anschließend reagiert der ISA Server auf ping-Anfragen aus dem Externen Netzwerk:

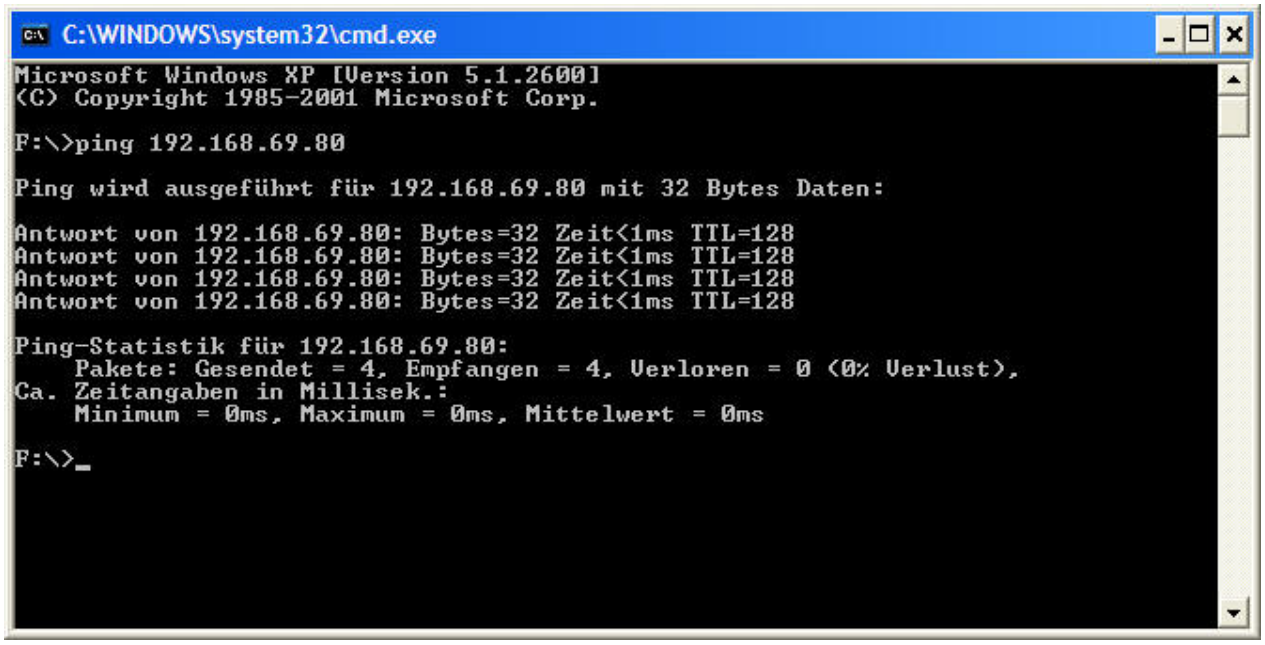


1b) Erstellen einer neuen Firewallrichtlinie

Das Erstellen einer Firewallrichtlinie wurde bereits in einem Artikel ausführlich erklärt. Daher wird hier nur die Zusammenfassung der neu erstellten Richtlinie gezeigt:

Die Protokolldefinition für Ping ist in der Toolbox unter "Infrastruktur" zu finden.

Nachdem die Änderungen übernommen wurde, lässt sich der ISA Server von extern anpingen:



Beachten Sie, dass bei beiden o.g. Konfigurationen sämtliche IP-Adressen, die auf der externen Schnittstelle gebunden sind, angepingt werden können.

2. Konfiguration des ISA Server für ausgehende ping-Anfragen interner Clients

Für diesen Konfigurationsschritt ist wieder eine neue Firewallrichtlinie erforderlich:

Damit kann ein interner Rechner ein externes Ziel anpingen:

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Dokumente und Einstellungen\Administrator>ping 192.168.69.1

Ping wird ausgeführt für 192.168.69.1 mit 32 Bytes Daten:

Antwort von 192.168.69.1: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.69.1: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.69.1: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.69.1: Bytes=32 Zeit=2ms TTL=63

Ping-Statistik für 192.168.69.1:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 2ms, Maximum = 2ms, Mittelwert = 2ms

C:\Dokumente und Einstellungen\Administrator>
```

Zugriff auf Windowsupdate V5 durch den ISA 2004 - Von Christian Gröbner

---

Die Informationen in diesem Artikel beziehen sich auf:

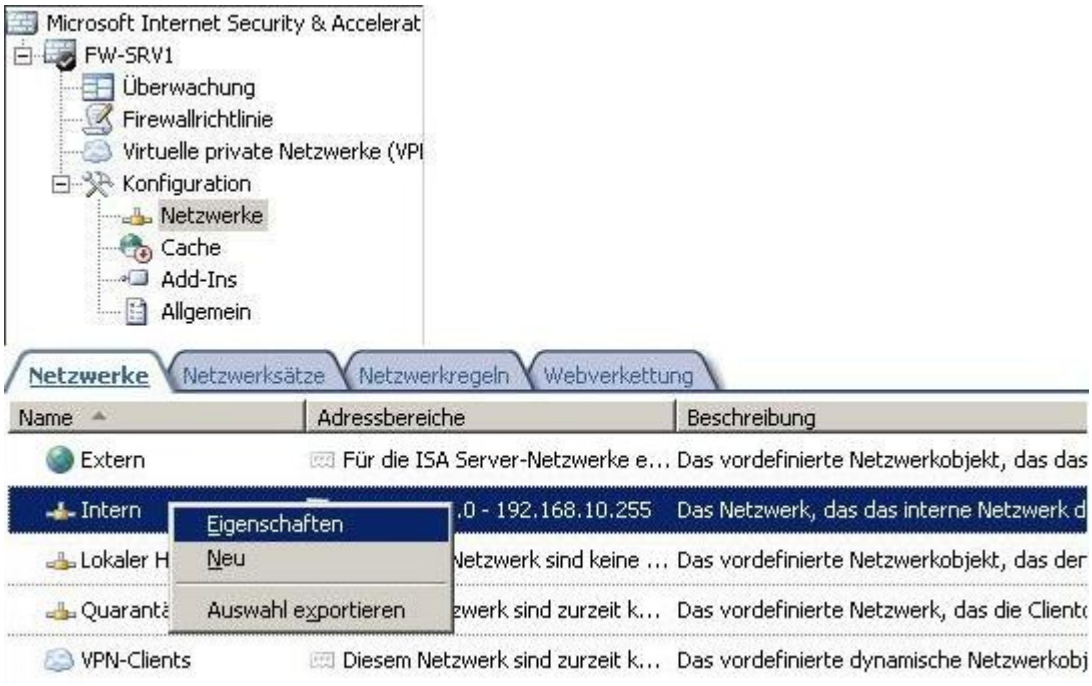
- Microsoft ISA Server 2004

Aufgrund von NTLM Autentifizierungsproblemen am Proxy schlägt das Windowsupdate V5 fehl. Damit der Zugriff reibungslos funktioniert, muss eine Firewallregel erstellt werden, die anonymen Zugriff auf die Windowsupdate Seiten erlaubt.

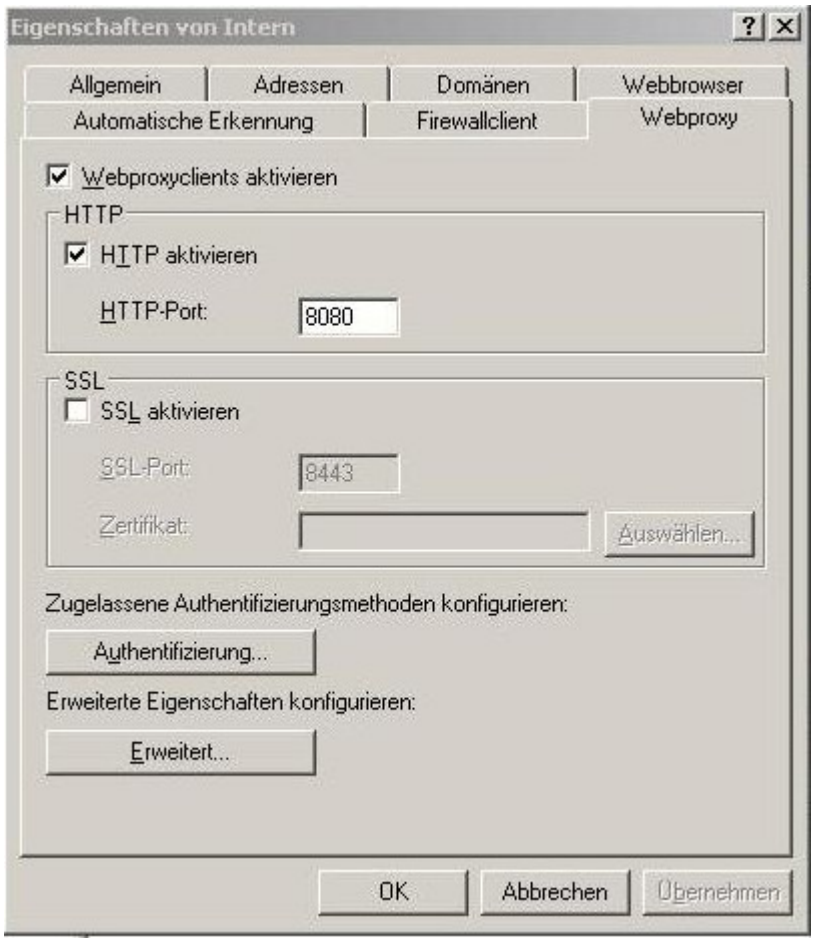
Hinweis: Dieses Problem tritt nur auf, falls Sie Authentifizierung am ISA für ausgehende Webanfragen fordern!

Wie Sie den ISA 2004 dafür konfigurieren, damit Ihre Konfiguration trotz anonymen Zugriff sicher bleibt, erfahren Sie in dieser Anleitung.

1. Deaktivierung der Webproxy Authentifizierung



Gehen Sie in die Eigenschaften des Netzwerkes, über das auf die Windowsupdate Seiten zugegriffen werden muss.

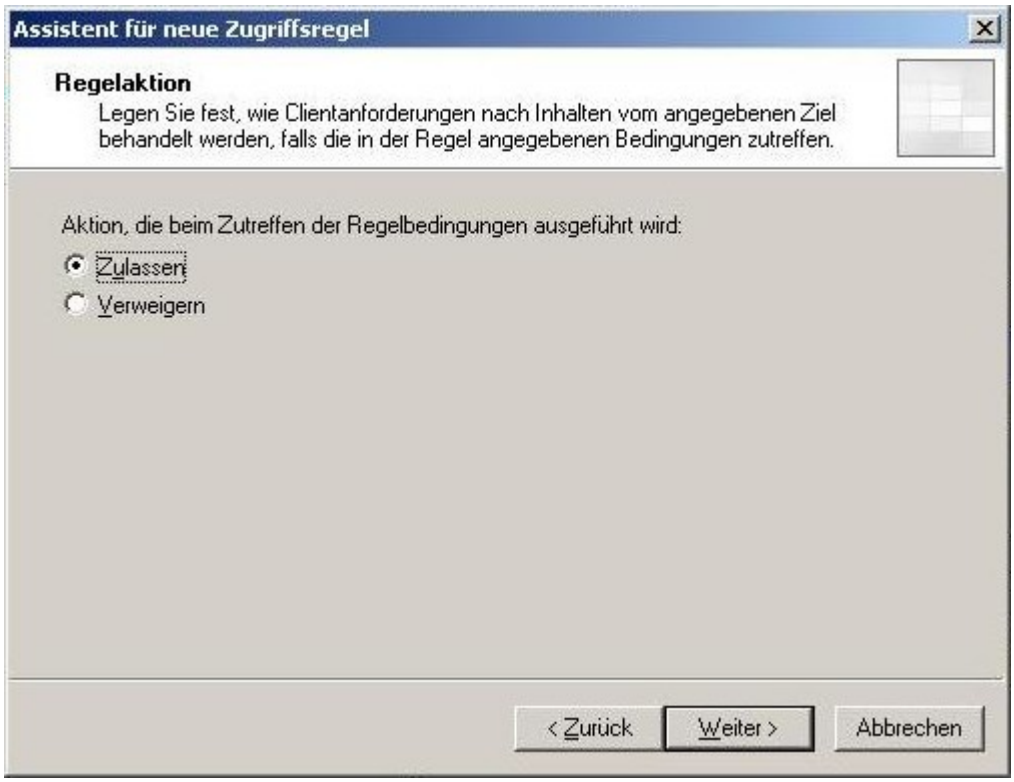


Öffnen Sie unter dem Karteireiter Webproxy die Authentifizierungsmethoden, über den Button Authentifizierung.

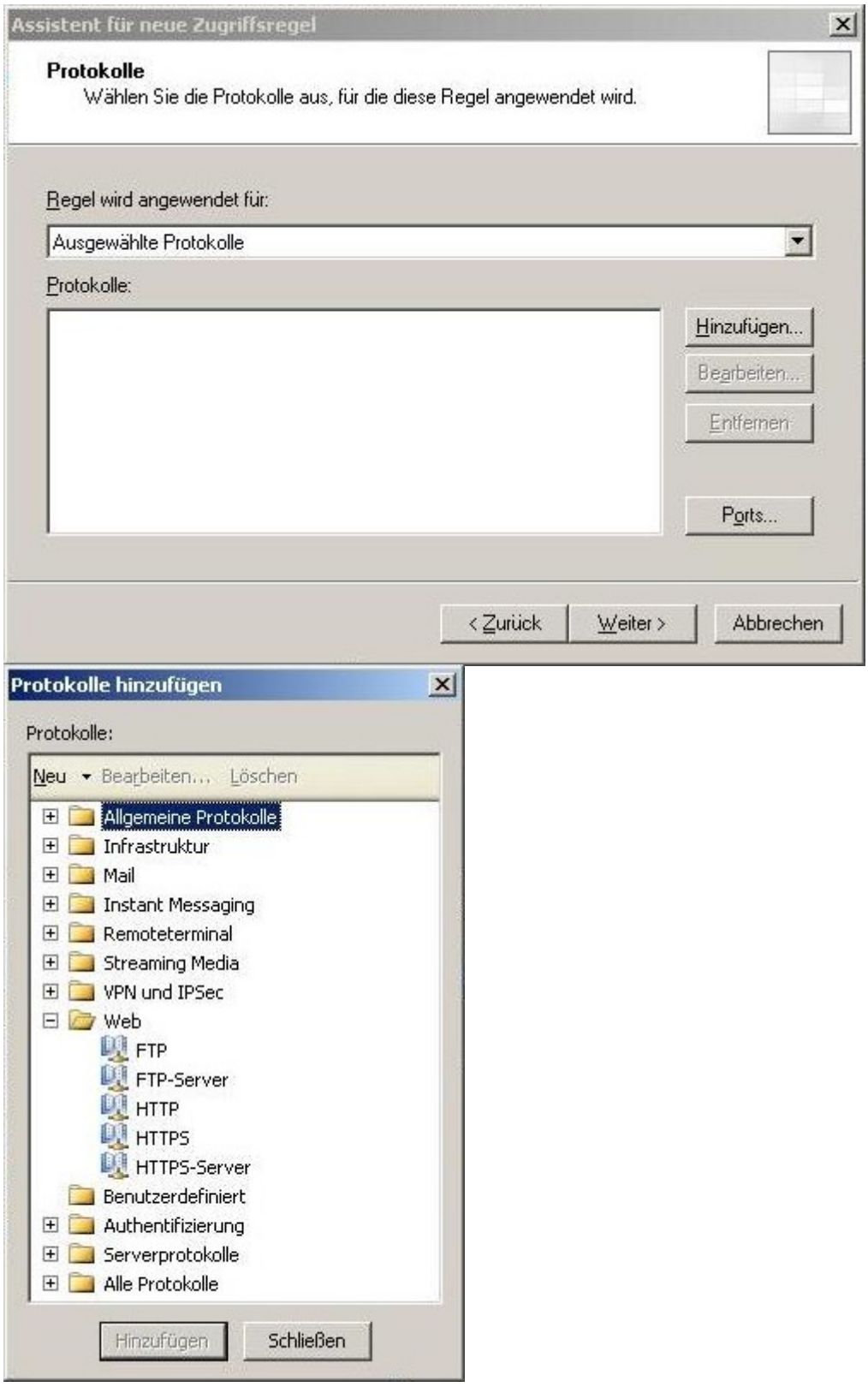
Entfernen Sie den Haken bei *Authentifizierung ist für alle Benutzer erforderlich*, um die generelle Authentifizierung auf Benutzerebene zu deaktivieren. Falls Sie Authentifizierung für den Webzugriff fordern wollen, müssen Sie die entsprechenden Benutzer bzw. Gruppen direkt in der Firewallrichtlinie für den Webzugriff angeben.

2. Erstellen einer Firwallrichtlinie für den anonymen Zugriff

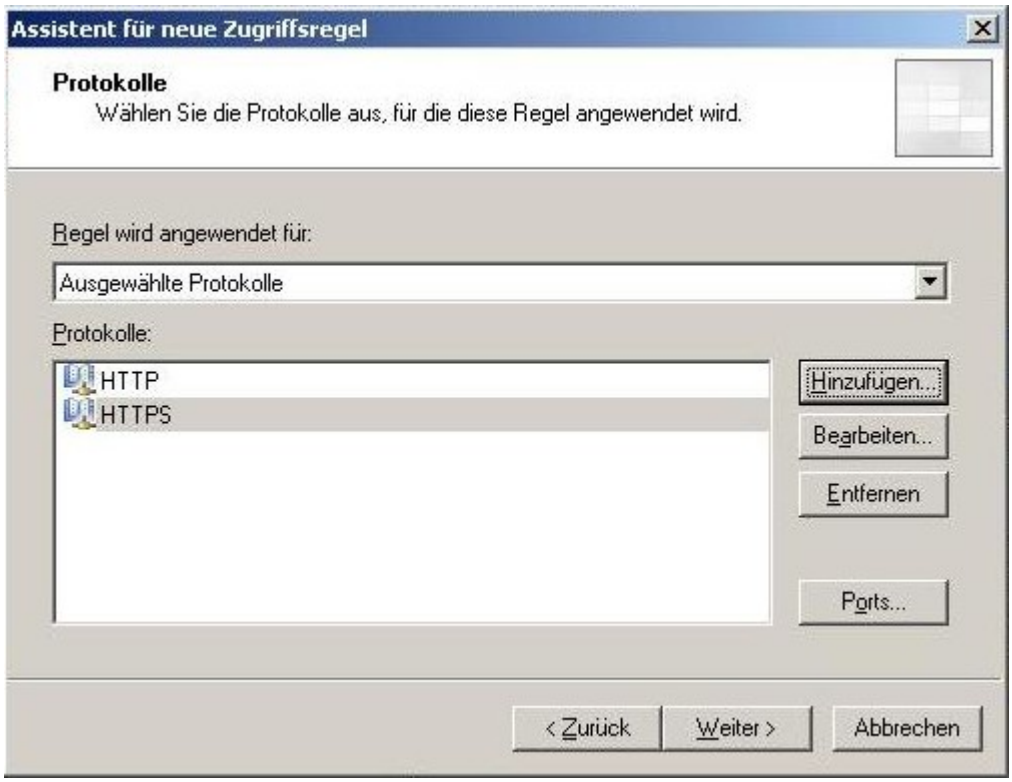
Erstellen Sie über Firewallrichtlinien -> Neu -> Zugriffsregel eine neue Firewallrichtlinie. Es öffnet sich der Assistent zur Erstellung einer neuen Firewallrichtlinie. Vergeben Sie zunächst einen Namen für die Regel.



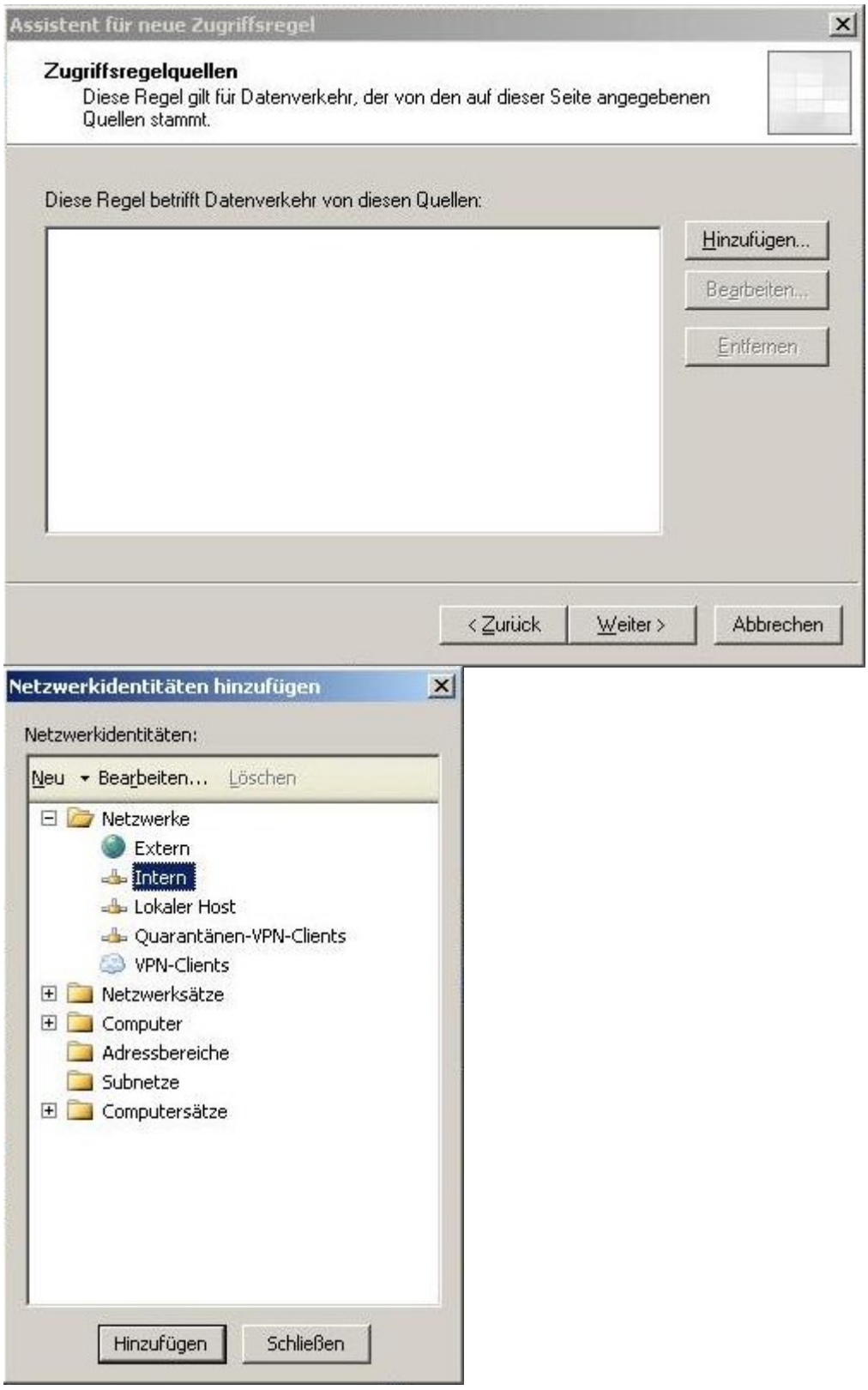
Als Aktion wählen Sie Zulassen aus, um den Zugriff zu gewähren.



Ändern Sie unter *Regel wird angewendet für* die Auswahl auf *Ausgewählte Protokolle* ab und fügen diese über den
Button Hinzufügen hinzu. Für den Zugriff auf das Windowsupdate V5 werden die Protokolle HTTP und HTTPS, unter der Kategorie
Web, benötigt

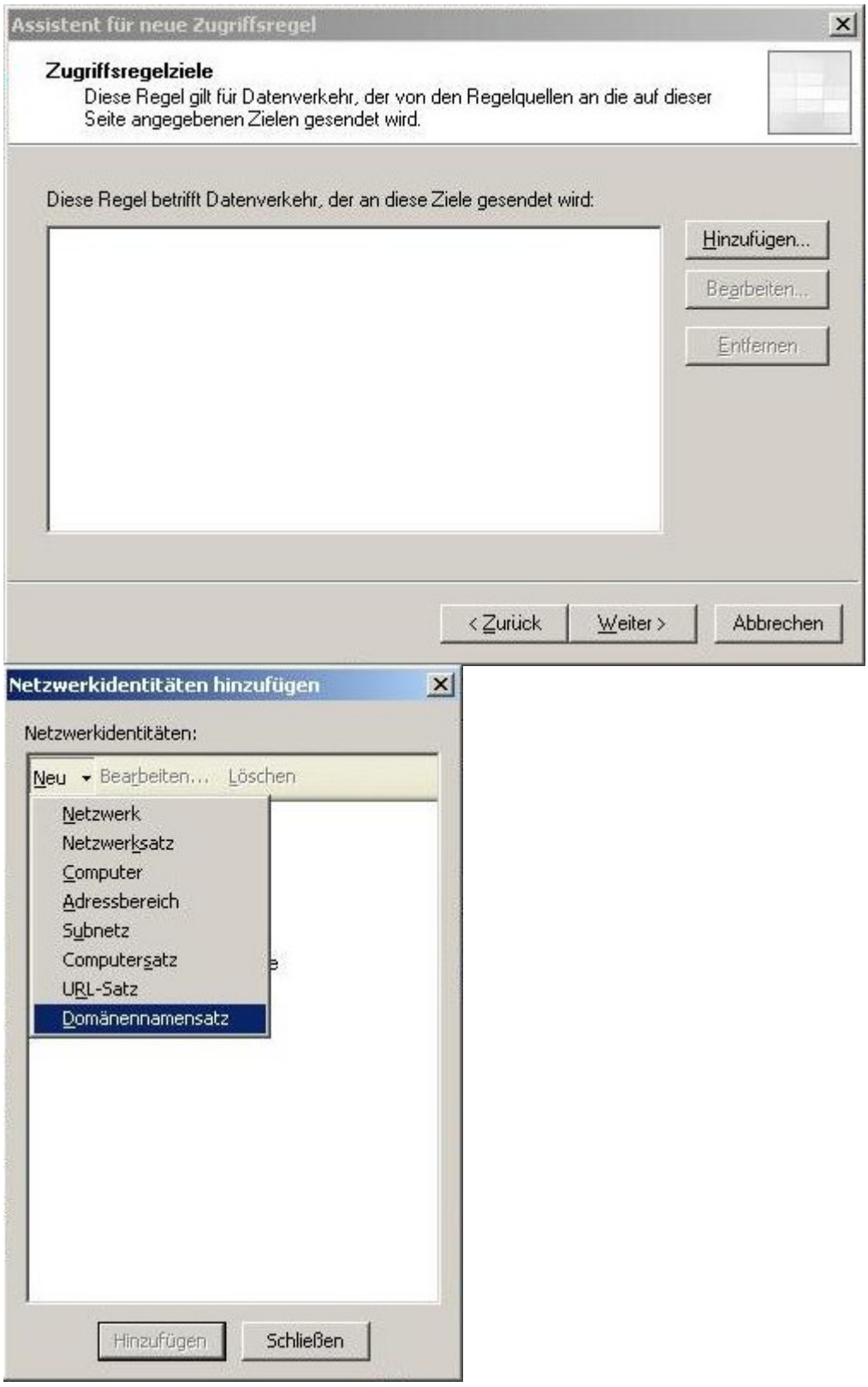


Nachdem Sie die Protokolle ausgewählt haben, sollte die Auswahl der Protokolle wie oben abgebildet aussehen.

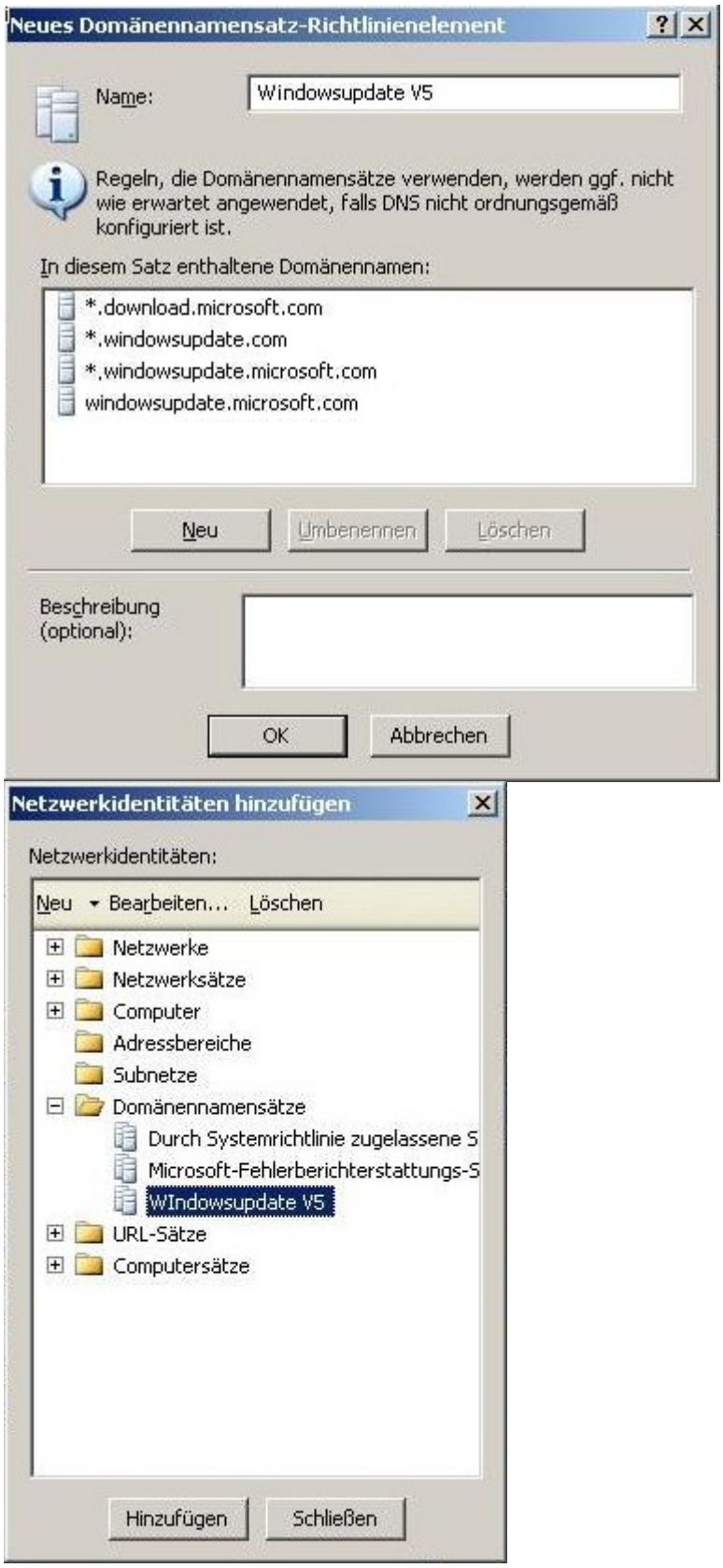


Sie müssen angeben, aus welchem Netzwerk der Zugriff gewährt wird. Fügen Sie hier, über den Button Hinzufügen, alle Netz-
werke, die Zugriff benötigen, der Regel hinzu. Wählen Sie unter der Kategorie Netzwerke die Netzwerke aus, die Sie der
Regel hinzufügen wollen.

Anschließend sollten als Zugriffsquellen nur die Netzwerke ausgewählt sein, die Zugriff benötigen.



Fügen Sie über den Button Hinzufügen das Ziel der Regel hinzu. Erstellen Sie über Neu -> Domänennamensatz ein neues Regelelement um den Zugriff auf bestimmte externe Ziele zu beschränken.



Vergeben Sie einen Namen und fügen Sie über Neu folgend angegebene Domänen hinzu und wählen Sie den eben erstellten Domänennamensatz unter der Kategorie Domänennamensätze aus.

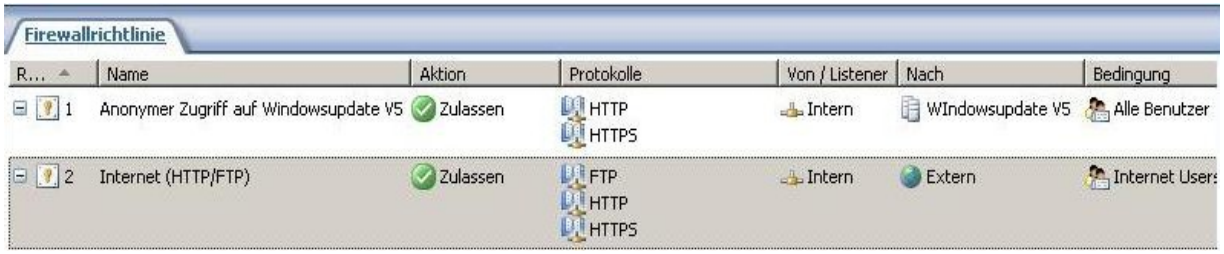
Benötigte Domänen für Windowsupdate V5:

- *.download.microsoft.com
- *.windowsupdate.com
- *.windowsupdate.microsoft.com
- windowsupdate.microsoft.com

Als externes Zugriffsziel sollte nur der Domänennamensatz ausgewählt sein.

Diese Regel muss für alle Benutzer gelten, da ein anonymer Zugriff benötigt wird. Deshalb wurde der Zugriff durch einen Domänennamensatz beschränkt um nicht den gesamten Zugriff auf das Internet anonym zu gewähren.

Abschließend bekommen Sie alle Einstellungen als Zusammenfassung angezeigt.



Setzten Sie die Regel für den Zugriff auf die Windowsupdate Seiten in der Reihenfolge vor die Regel die den Internetzzugriff
erlaubt. Ansonsten hätte diese Regel Vorrang und somit wäre kein anonymer Zugriff möglich, da in der Regel für den Internet-
zugriff Authentifizierung auf Benutzerebene gefordert wird.

ISA Server 2004 – Microsoft SQL Server Veröffentlichung

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Dieser Artikel beschreibt die Veröffentlichung eines Microsoft SQL Server 2000 über einen ISA Server 2004.

Der Microsoft SQL Server 2000 mit SP3a befindet sich im internen Netzwerk und soll über ein externes Netzwerk erreichbar sein.
Bei dem externen Netzwerk handelt es sich um ein geschlossenes Netzwerk zum Anschluss einer bundesweit agierenden Firma mit diversen Zweigstellen.
Warum dieser Hinweis: Wenn Sie mit dem Gedanken spielen, einen MS SQL Server über das Internet zu veröffentlichen, kann ich Ihnen diese Vorgehensweise definitiv ***NICHT*** empfehlen, da der MS SQL Server quasi direkt am Internet hängt. Für den Zugriff von ***EXTERN*** auf einen MS SQL Server im LAN, verwenden Sie sichere Verbindungen wie VPN.
Details zum Thema VPN finden Sie hier und hier.

Die Installation eines MS SQL Server 2000 mit SP3a wird in diesem Artikel nicht beschrieben und vorausgesetzt.

Dieser Artikel wird in zwei Konfigurationsschritte unterteilt:

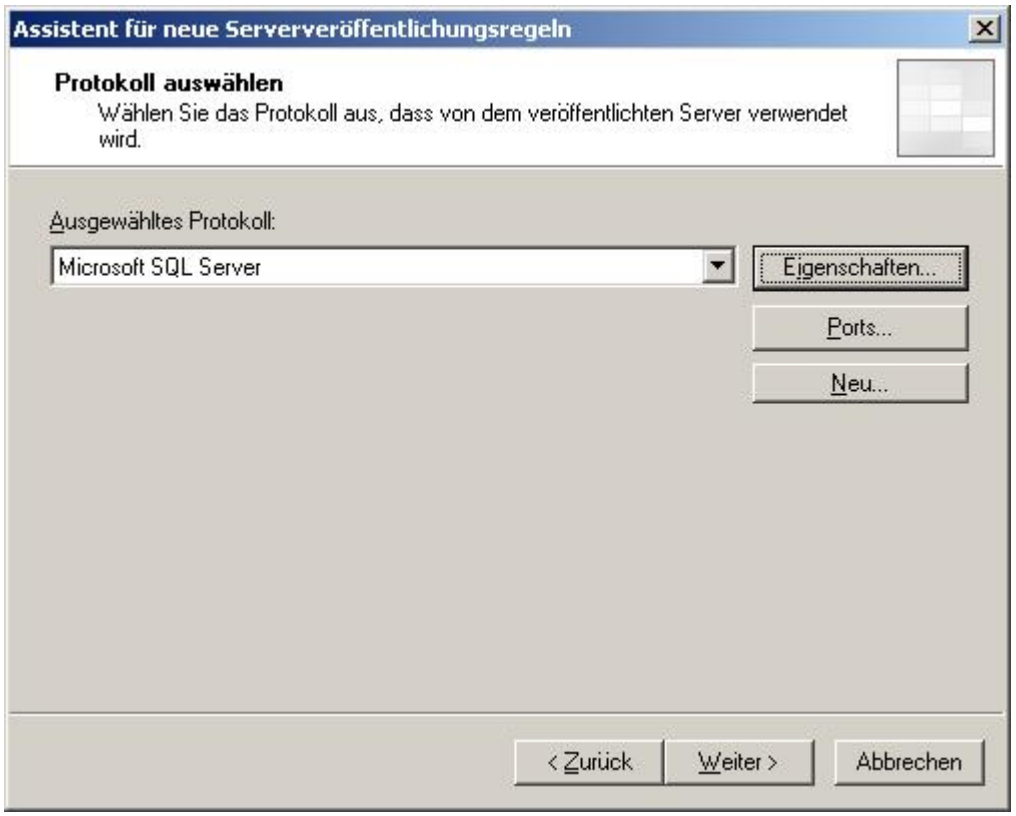
- Serververöffentlichung
- Client-Konfiguration

Serververöffentlichung

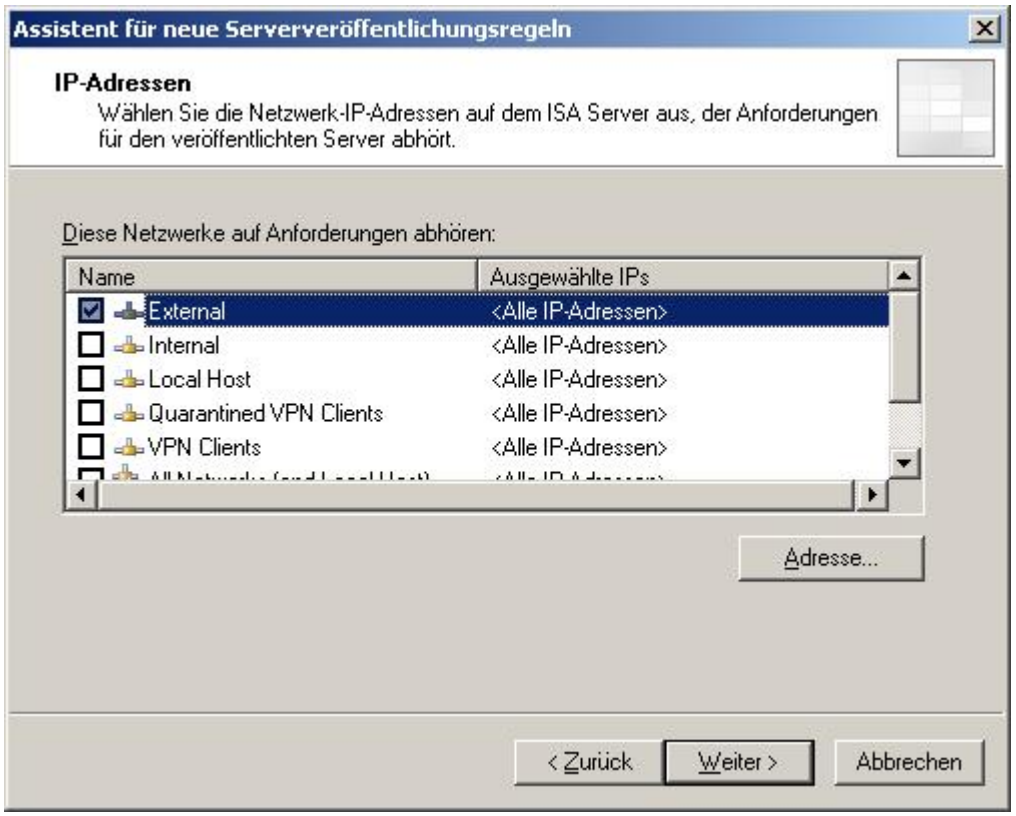
Als erstes müssen Sie eine Serververöffentlichung für den MS SQL Server erstellen. Klicken Sie dazu in der ISA Server Verwaltungskonsole mit der rechten Maustaste auf ***Firewallrichtlinie*** und wählen Sie ***Serververöffentlichungsregel*** aus.

Wählen Sie einen Namen für die neue Serververöffentlichungsregel.

Microsoft SQL Server 2004 bietet ein vordefiniertes Protokoll mit dem Namen ***Microsoft SQL Server***, welches den TCP Port 1433 Eingehend definiert. Wählen Sie das Protokoll aus dem Dropdown Feld aus.



Wählen Sie das Netzwerk aus, auf welchem der ISA Server 2004 auf Anfragen reagieren soll. Wir wählen das Netzwerk ***External*** aus.

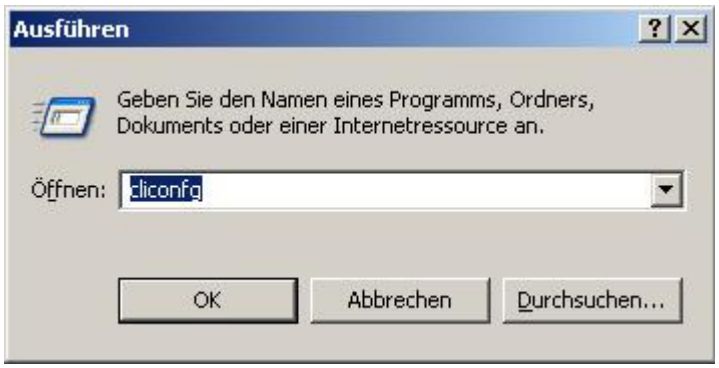


Überprüfen Sie die korrekten Einstellungen des Wizards.

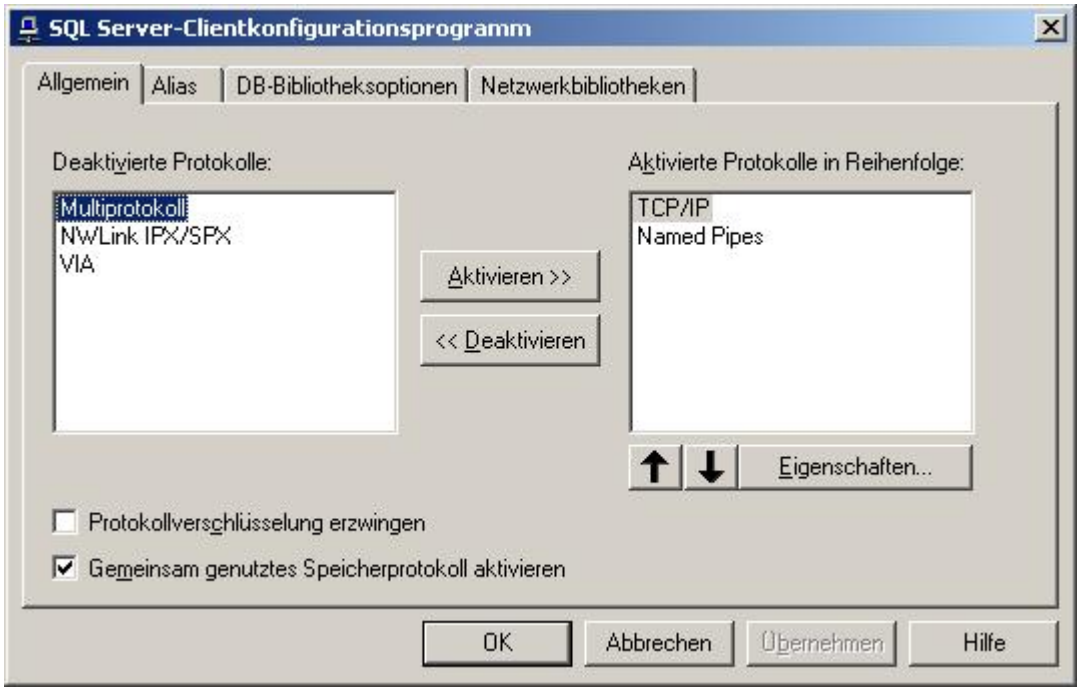
Der Serververöffentlichungswizard hat folgende Regel erstellt:

Clientkonfiguration

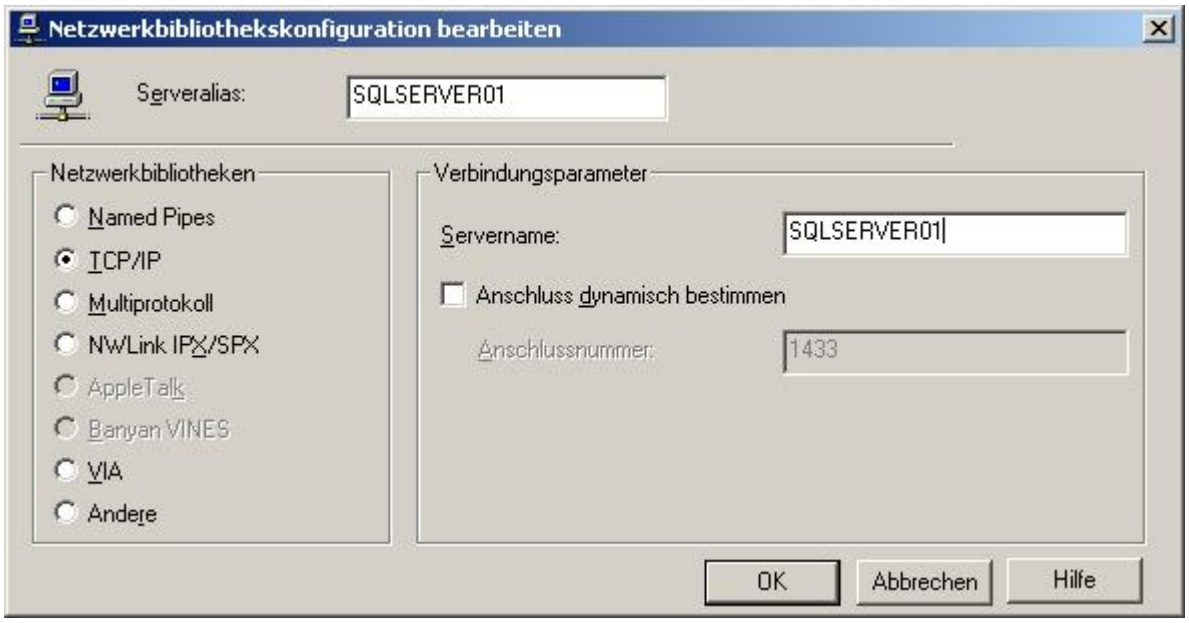
Der Microsoft SQL Server verwendet für die Kommunikation per Default nicht nur den Port 1433. Standardverbindungen verwenden Named Pipes. Bei der Verwendung von Named Pipes werden die Kommunikationsports dynamisch ausgehandelt (Ports >1024). Diese Art der Verbindung ist nicht für Firewalls geeignet.
Damit der Client (z. B. SQL Server Enterprise Manager) immer über Port 1433 mit dem internen MS SQL Server kommuniziert, müssen Sie die Konfiguration auf dem Client anpassen.
Starten Sie dazu das SQL Server Clientkonfigurationsprogramm - über ***Start - Ausführen - CLICONFG***. Das SQL Server Clientkonfigurationsprogramm ist Bestandteil der Microsoft SQL Server Client Installation.



Stellen Sie sicher, dass im Fenster ***Aktivierte Protokolle in Reihenfolge***, dass ***TCP/IP*** Protokoll an erster Stelle steht.



Klicken Sie jetzt auf den Reiter ***Alias*** auf ***Hinzufügen***, um einen neuen Alias für den MS SQL Server zu erstellen.
Tragen Sie im Feld ***Serveralias*** den Namen des MS SQL Servers ein, ebenso im Feld ***Servername*** im Bereich ***Verbindungsparameter***.
Im Bereich ***Netzwerkbibliothek*** wählen Sie ***TCP/IP*** aus und deaktivieren den Haken ***Anschluss dynamisch bestimmen*** im Bereich ***Verbindungsparameter***.



Die Konfiguration ist fertig. Sie können jetzt eine Verbindung mit dem internen MS SQL Server herstellen.

Einrichtung von RPC over HTTPS mit dem ISA Server 2004

Die Informationen in diesem Artikel beziehen sich auf:

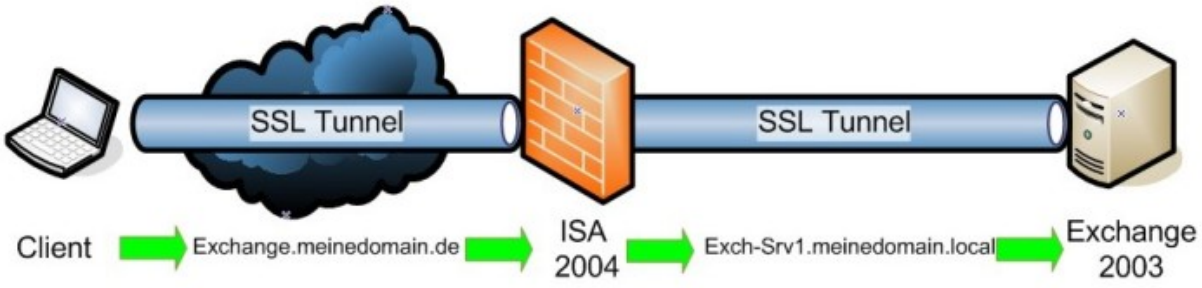
- Microsoft ISA Server 2004
- Microsoft Exchange Server 2003 SP1
- Microsoft Windows Server 2003

Der ISA Server 2004 bietet, wie schon der ISA Server 2000, viele Möglichkeiten von Extern auf sein Exchange Postfach zu zugreifen. Durch RPC over HTTPS besteht eine sichere Methode den internen Exchange Server zu veröffentlichen. Hierbei ist es nicht notwendig, wie bei einer reinen RPC Veröffentlichung, den kritischen Port 135 zu öffnen, da die RPC Pakete in einem SSL Tunnel übertragen werden. Die Pakete werden an den RPC über HTTP Proxy übermittelt, von dem der HTTP Header entfernt wird, und die reinen RPC Pakete an den Exchange Server weitergeleitet werden. Daten vom Exchange Server aus werden zuerst an den RPC über HTTP Proxy gesendet und von dort aus wieder als verschlüsselte HTTP Pakete an den Client weitergeleitet.

Vorteile dieser Verbindungsmethode sind:

- Die Benutzer arbeiten in der gewohnten Microsoft Outlook Umgebung
- Es besteht nur Zugriff auf den Exchange Server und nicht auf andere interne Ressourcen
- Aus einem Remote Netzwerk mit Firewall muss nur das Protokoll HTTPS erlaubt sein
- RPC over HTTPS funktioniert auch bei einem Small Business Server 2003

Szenario



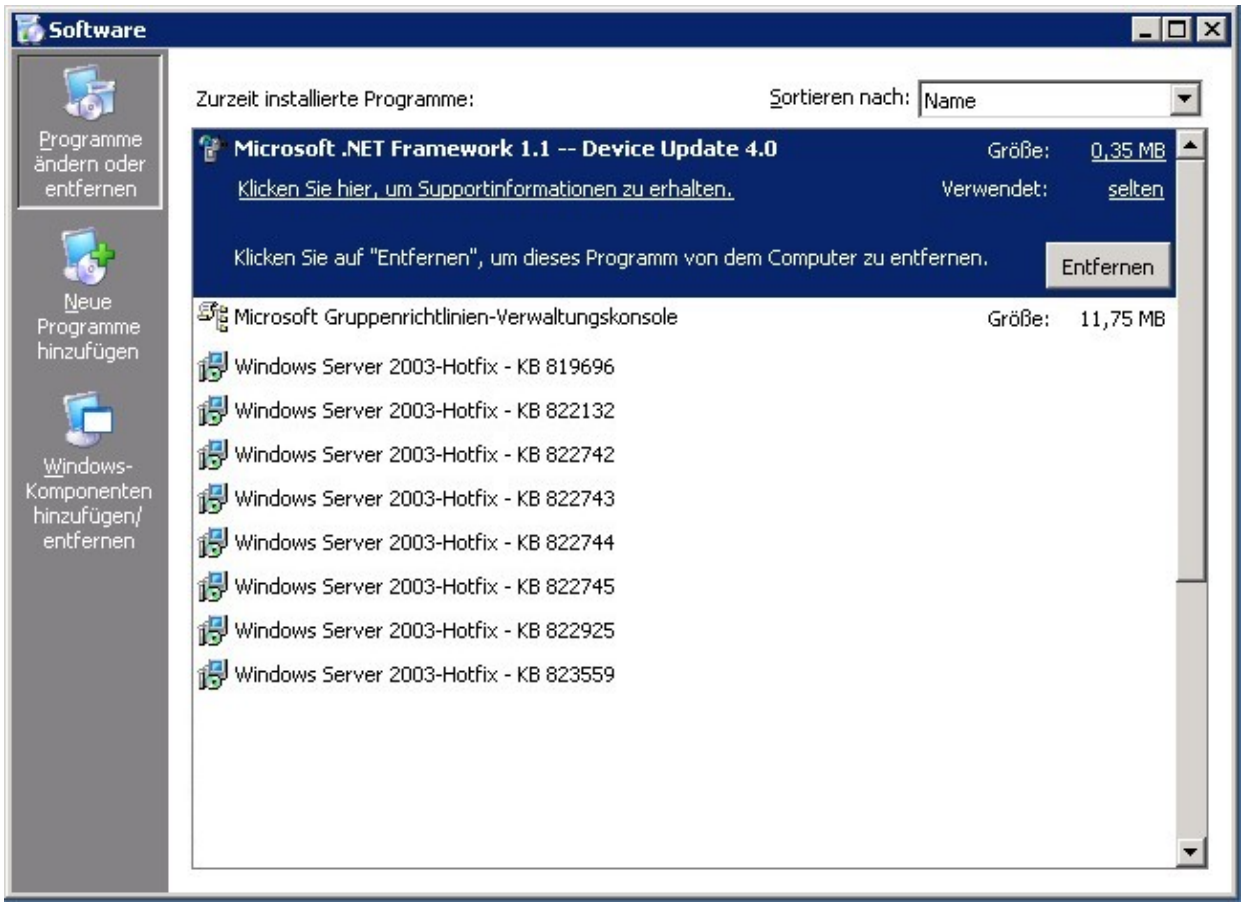
In dieser Anleitung wird die Verbindung zum Exchange Server mittels SSL Bridging hergestellt, d.h. es besteht ein SSL Tunnel zwischen dem Client und dem ISA Server und ein neuer Tunnel zwischen dem ISA- und dem Exchange Server. Hierzu sind zwei Webserverzertifikate für die SSL Verbindung notwendig. Ein Zertifikat für die Verbindung vom Client zum ISA Server für exchange.meinedomain.de, auf dem ISA Server, und intern für die Verschlüsselung vom ISA- zum Exchange Server für exch-srv1.meinedomain.local, auf dem Exchange Server. Wichtig hierbei ist, dass der Client der Zertifizierungsstelle für das externe Zertifikat und der ISA Server der Zertifizierungsstelle des internen Zertifikates vertrauen. Des Weiteren müssen die FQDN's (Full Qualified Domain Name) mit denen der Zertifikate übereinstimmen und die Zertifikate dürfen nicht abgelaufen sein, ansonsten kommt

kein Verbindungsaufbau zustande.

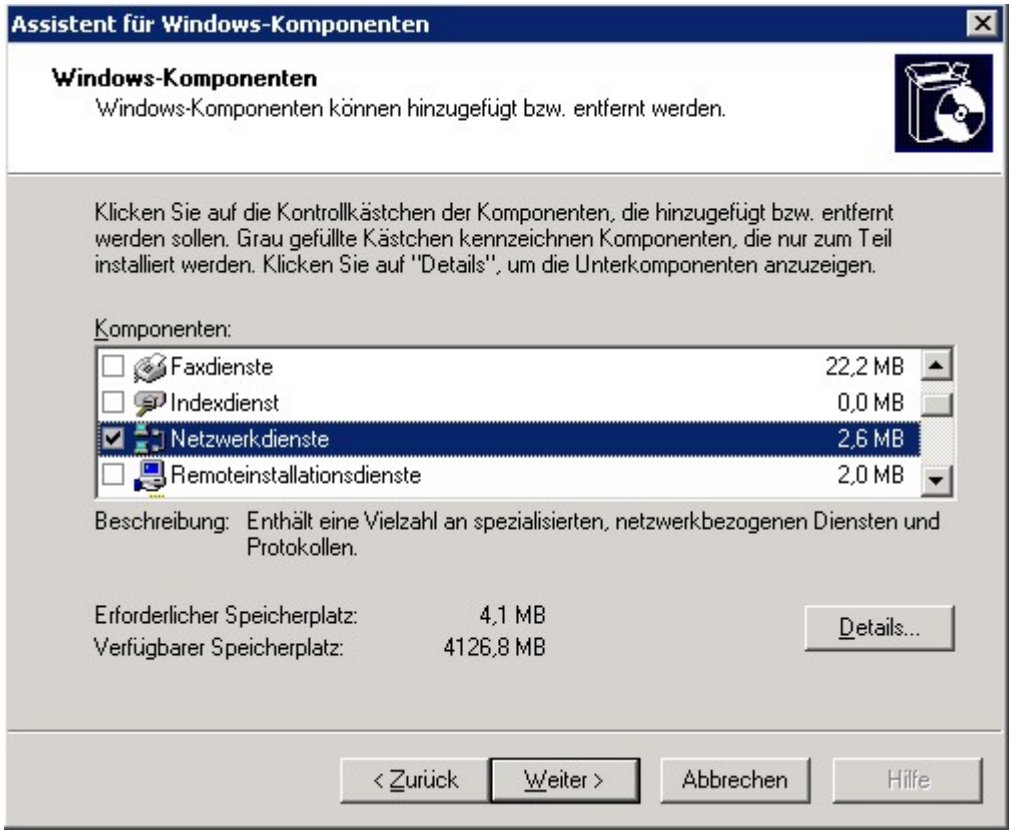
Voraussetzungen:

- Exchange Server 2003 SP1 auf einem Windows 2003 Server
- Active Directory auf Windows 2003 Server
- Ein Webserverzertifikat für exchange.meinedomain.de dem ISA Server
- Ein Webserverzertifikat für exchange.meinedomain.local auf dem Exchange Server
- Windows XP SP1 mit Patch 331320 oder SP2
- Outlook 2003

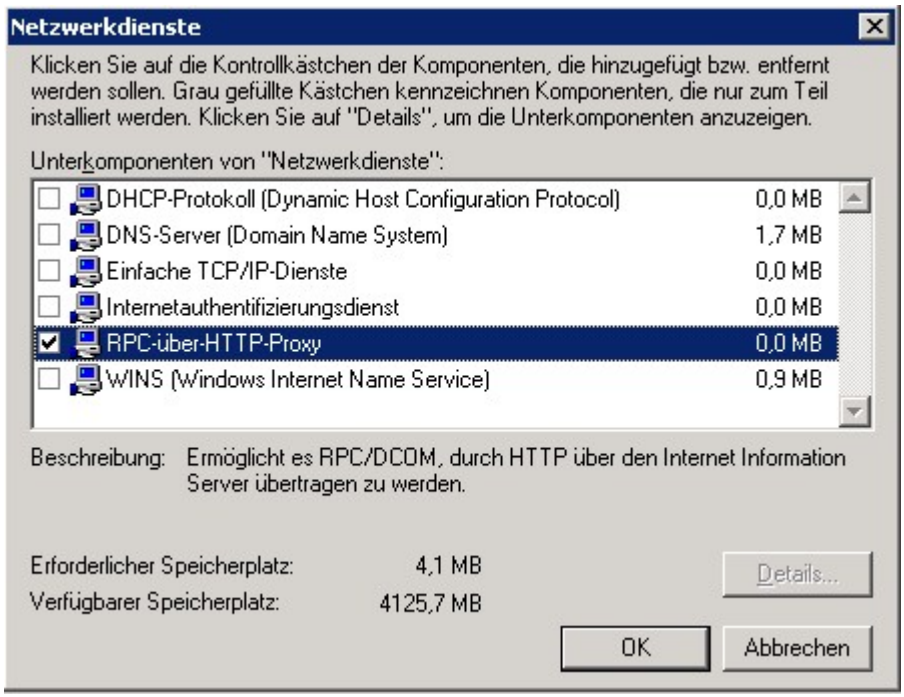
1. Installation des RPC over HTTP Proxys



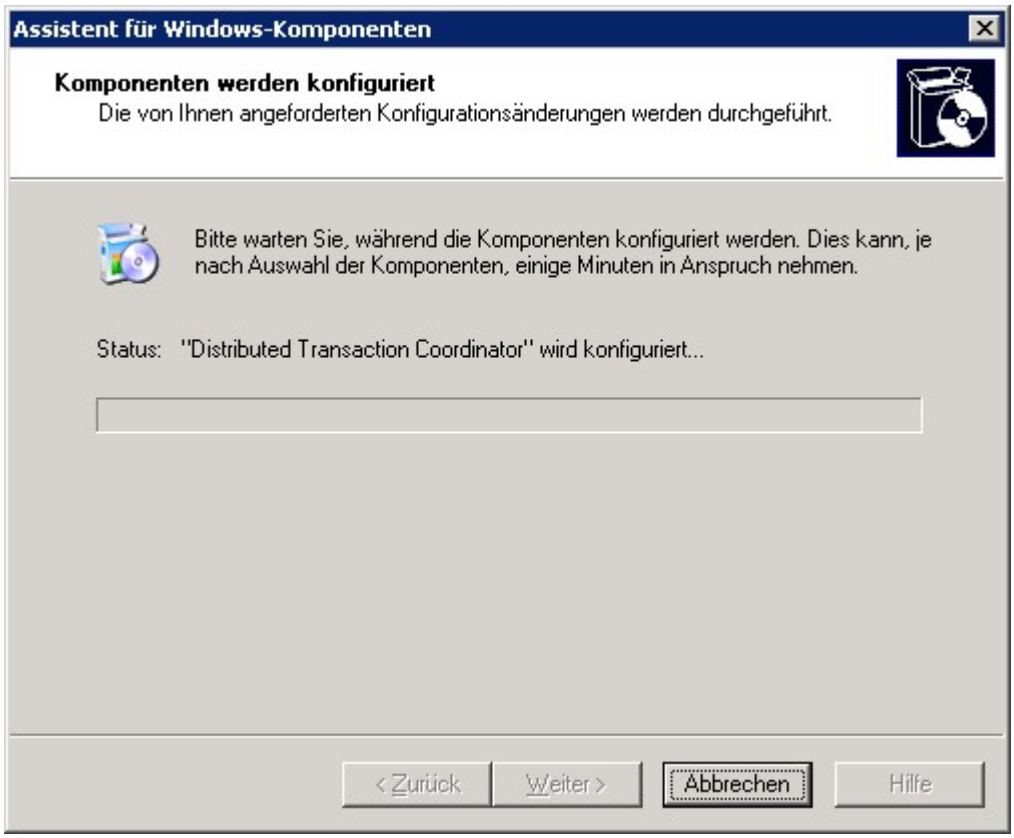
Öffnen Sie hierzu die Softwareverwaltung über Start -> Programme -> Systemsteuerung -> Software und klicken auf Windowskomponenten hinzufügen/entfernen.



Unter Komponenten wählen Sie die Netzwerkdienste aus und klicken auf Details.



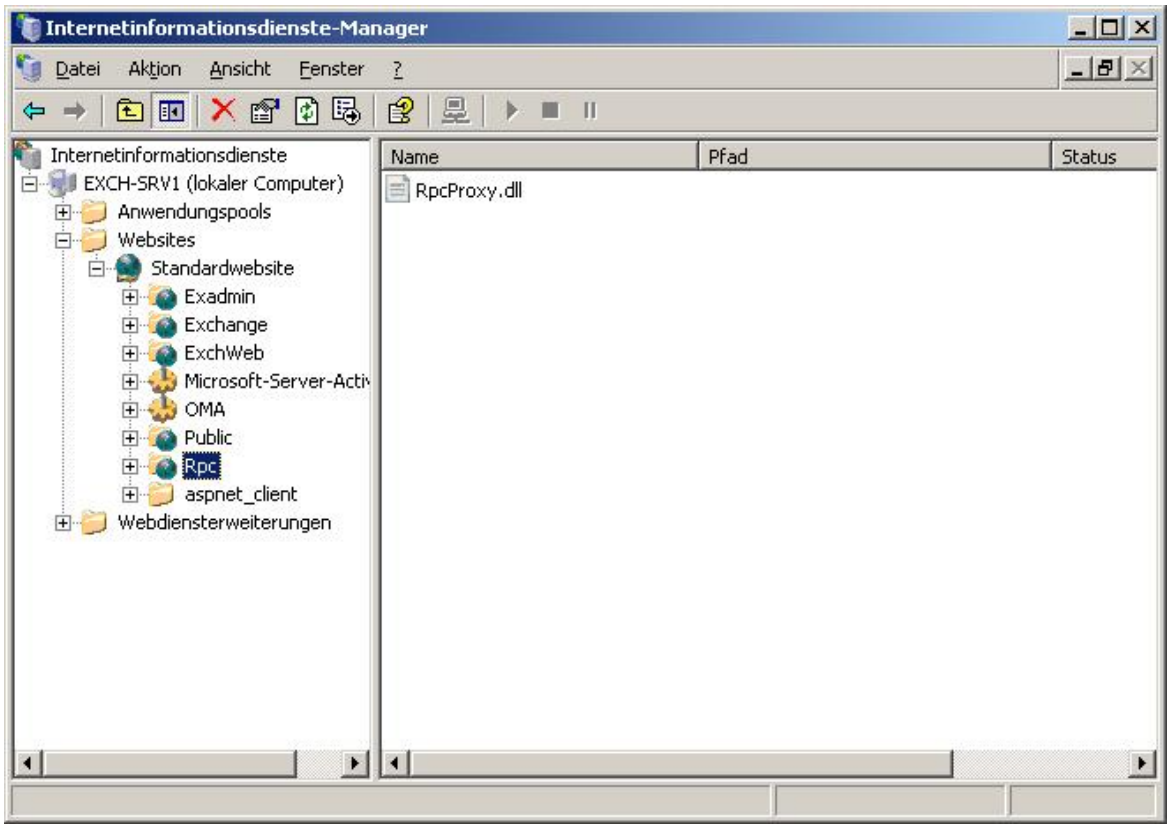
Wählen Sie hier die Option RPC-über-HTTP Proxy aus.



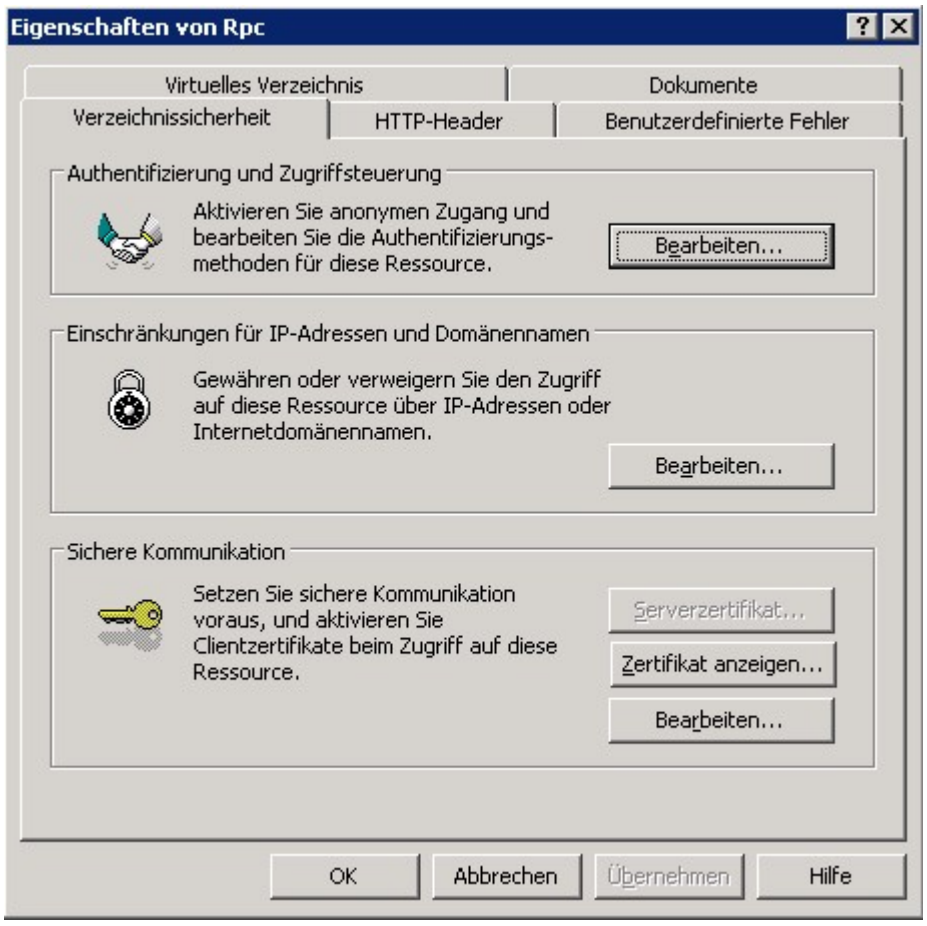
Anschließend wird der RPC-über-HTTP Proxy installiert.

Schließen Sie die Installation mit Fertigstellen ab.

2. Konfiguration des virtuellen RPC Verzeichnisses

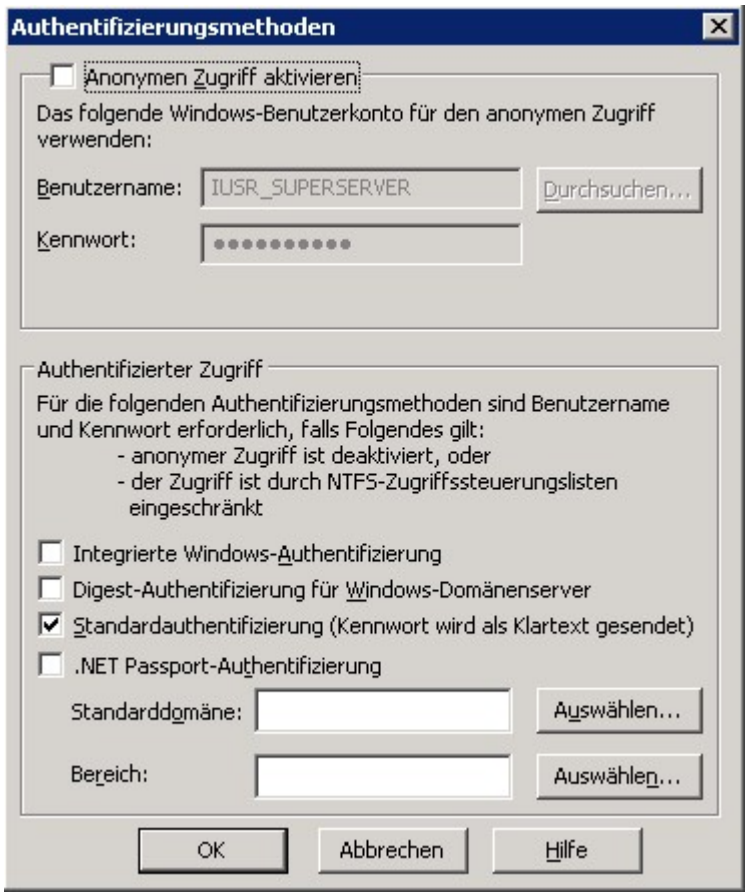


Öffnen Sie den Internetinformationsdiente-Manager über Start -> Programme -> Verwaltung und öffnen Sie Eigenschaften des RPC Verzeichnisses.

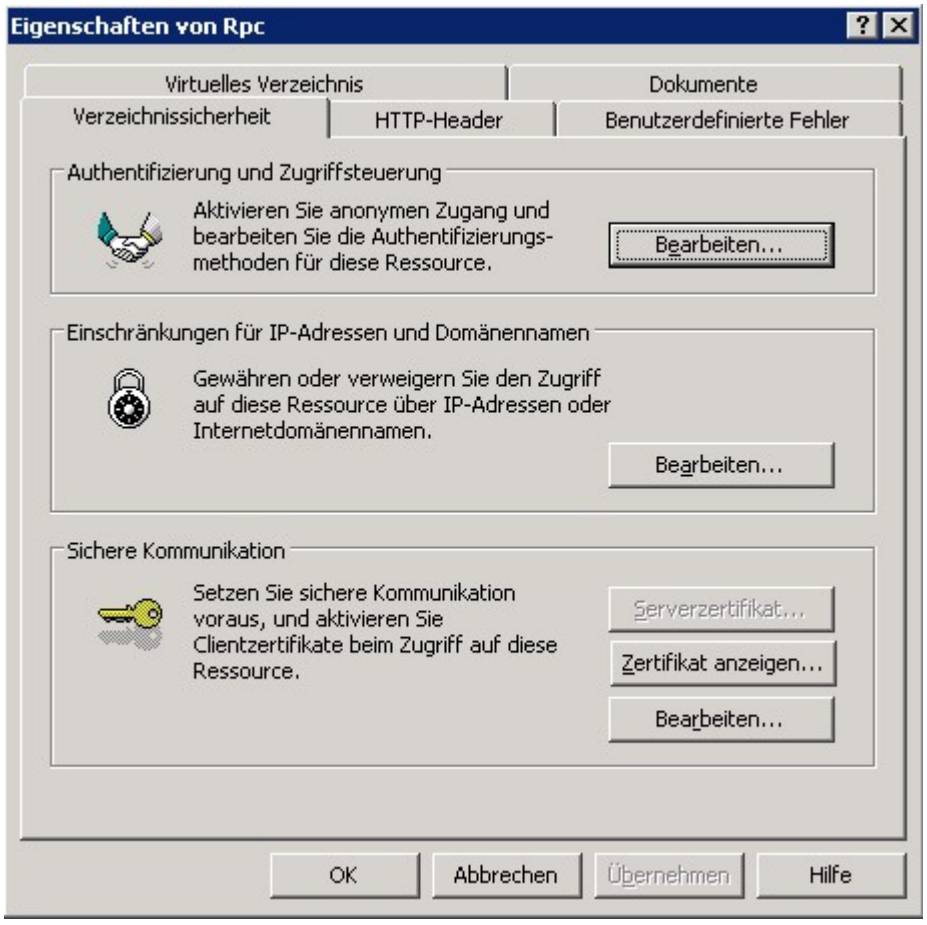


Konfigurieren Sie die Authentifizierungsmethoden, indem Sie über die Option "Authentifizierung und Zugriffsteuerung" auf Bearbeiten klicken.

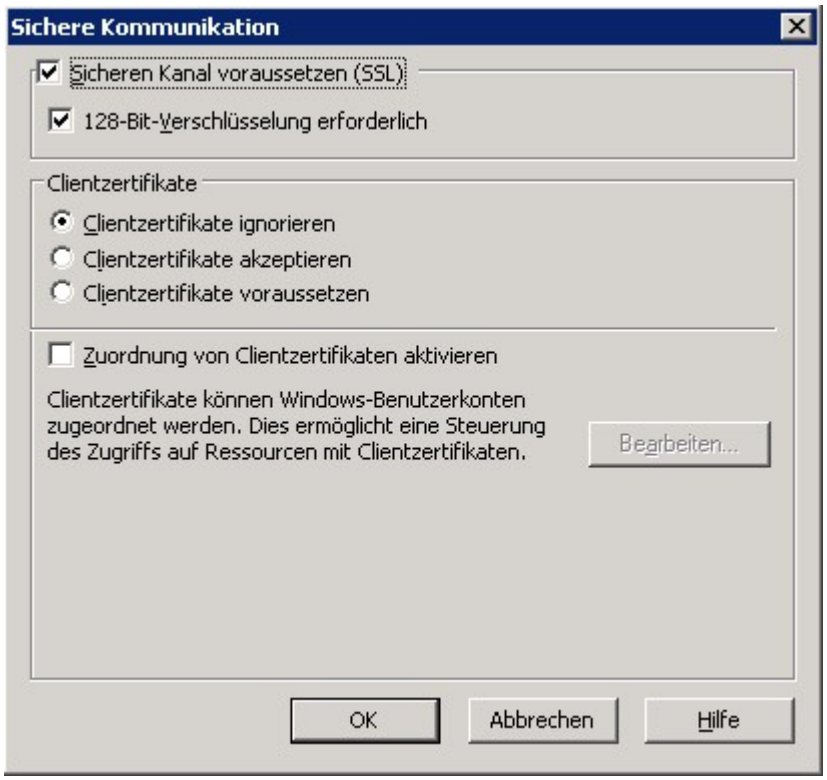
Wenn Sie noch kein Zertifikat für den Webserver besitzen können Sie unter Sichere Kommunikation ein Zertifikat anfordern. Wie Sie ein Zertifikat anfordern finden Sie in folgender Anleitung.



Deaktivieren Sie den anonymen Zugriff, indem Sie den Haken entfernen und wählen Sie als Authentifizierungsmethode die Standartauthentifizierung aus. Die Standartauthentifzierung ist hier kein Sicherheitsrisiko, da die Daten über einen SSL Tunnel transportiert werden. Übernehmen Sie die Einstellungen mit OK.



Konfigurierien Sie die Authentifizierung und Zugriffssteuerung über den Button Bearbeiten.



Wählen Sie Sicheren Kanal voraussetzen (SSL) aus, um nur SSL Anfrage zu zulassen. Optional kann eine Verschlüsselungsstärke von 128 Bit gefordert werden.

2.1 Konfiguration der Ports für die Kommunikation des RPC über HTTP Proxys

Hinweis: Folgende Schritte sind nicht notwendig, falls es sich um einen Small Business Server 2003 handelt, oder der Exchange Server auf einem Domänencontroller installiert ist.

Abschließend müssen Sie noch die Ports festlegen auf denen die Kommunikation mit dem RPC über HTTP Proxy statt findet.
Öffen Sie hierzu über Start -> Ausführen -> regedit den Registrierungseditior und navigieren Sie zu folgednem Pfad:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy

Ändern Sie den Wert des Registrierungsschlüssels ValidPorts in folgenden Wert ab:

NETBIOS-Name des Servers:6001;FQDN des Servers:6001;NETBIOS-Name des Servers:6004;FQDN des Servers:6004

In dieser Anleitung entspricht das:

exch-srv1:6001;exch-srv1.meinedomain.local:6001;exch-srv1:6004;exch-srv1.meinedomain.local:6004

Die Konfiguration am Exchange Server ist nun abgeschlossen.

3. Konfiguration der Globalen Katalog Server

Hinweis: Folgende Schritte sind nicht notwendig, falls es sich um einen Small Business Server 2003 handelt, oder der Exchange Server auf einem Domänencontroller installiert ist.

Um die Kommunikation zwischen dem RPC über HTTP Proxy und den Globalen Katalogen zu gewährleisten, müssen Sie die benötigten Ports angeben. Öffnen Sie wieder über Start ->Ausführen -> regedit den Registrierungseditor und navigieren Sie zu folgendem Pfad:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

und erstellen einen neunen Registrierungsschlüssel vom Typ *Wert der mehrteiligen Zeichenfolge* mit dem Namen *NSPI interface protocol sequences*. Als Wert für diesen Registrierungsschlüssel geben Sie *ncacn_http:6004* ein.

Wiederholen Sie diesen Schritt für jeden Globalen Katalog Server in Ihrem Netzwerk.

4. Konfiguration des ISA Servers

Am ISA Server selbst muss eine Sichere Webveröffentlichung erstellt werden, um die Anforderungen an den RPC über HTTP Proxy auf dem Exchange Server weiter zu leiten. Zusätzlich ist ein Zertifikat für die SSL Verschlüsselung notwendig, das an den Weblistener gebunden werden muss.

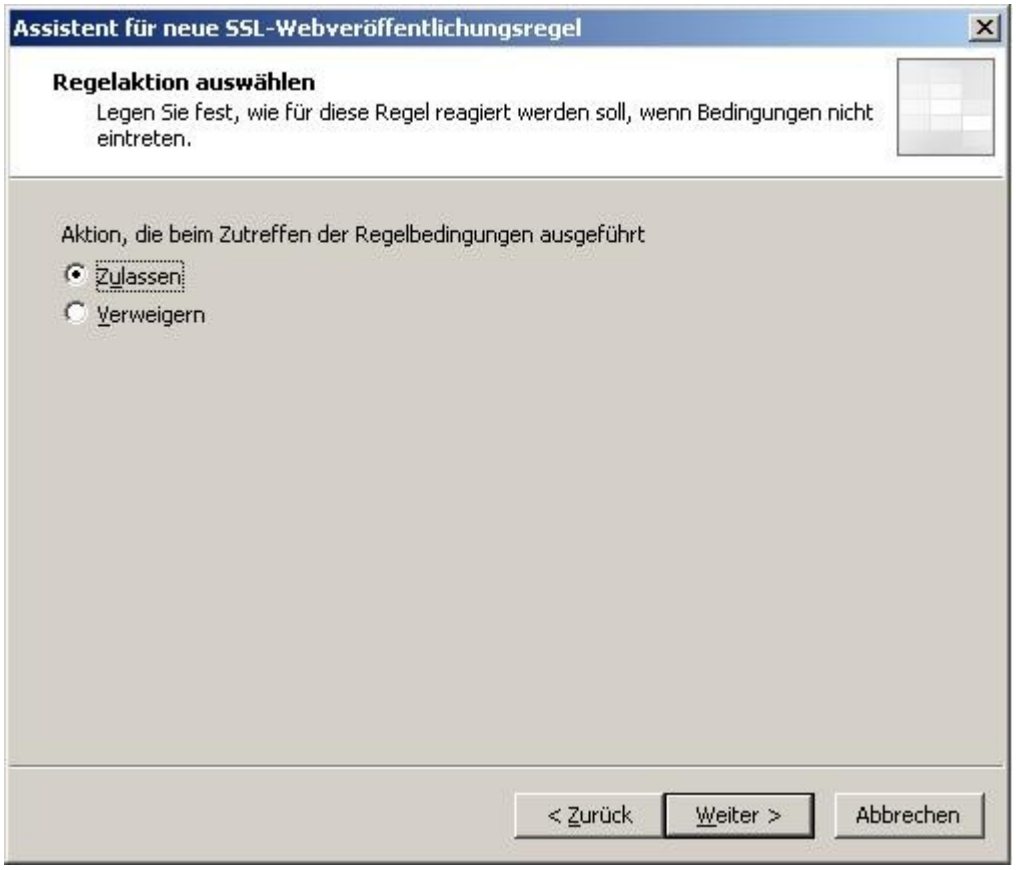
Wie Sie ein Zertifikat am ISA importieren finden Sie unter folgender Anleitung:

- OWA SSL Teil 3

4.1 Erstellen einer Sicheren Webserververöffentlichung (Teil 1)

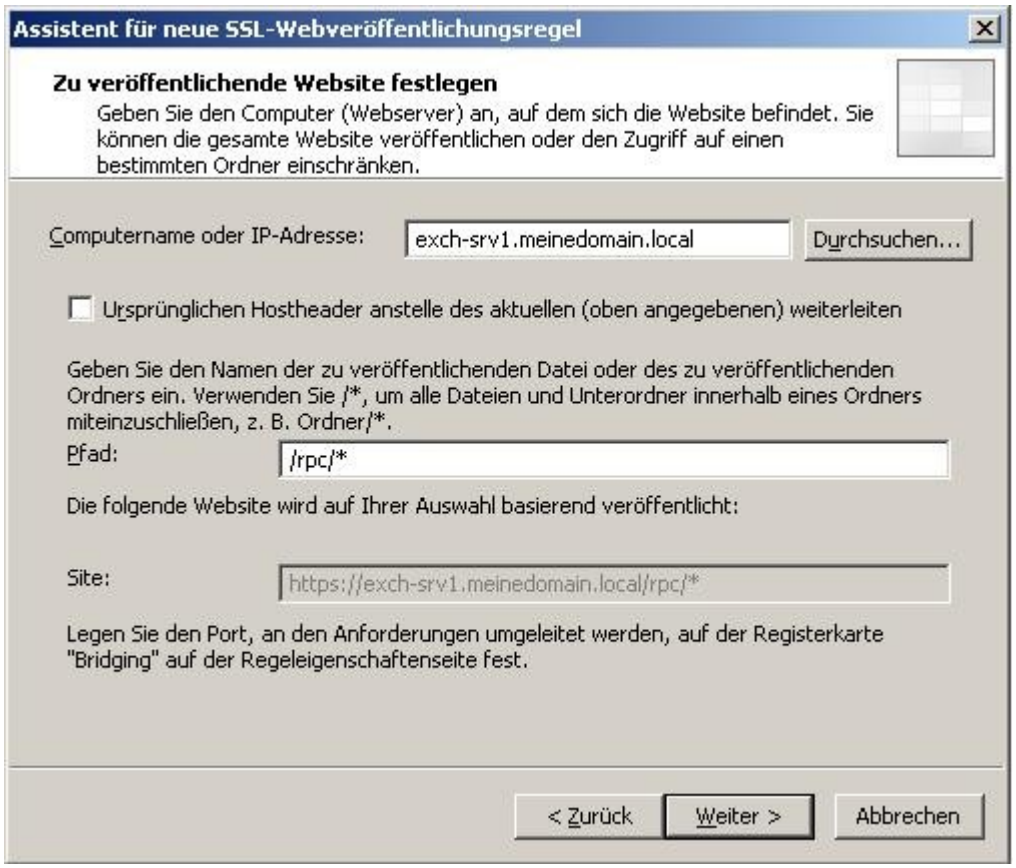
Erstellen Sie über Servername -> Firewallregeln -> Neu -> Sichere Webserververöffentlichung eine neue Firewallregel.

Wählen Sie die Option SSL-Bridging, damit die gesamte Kommunikation über einen SSL Tunnel statt findet.



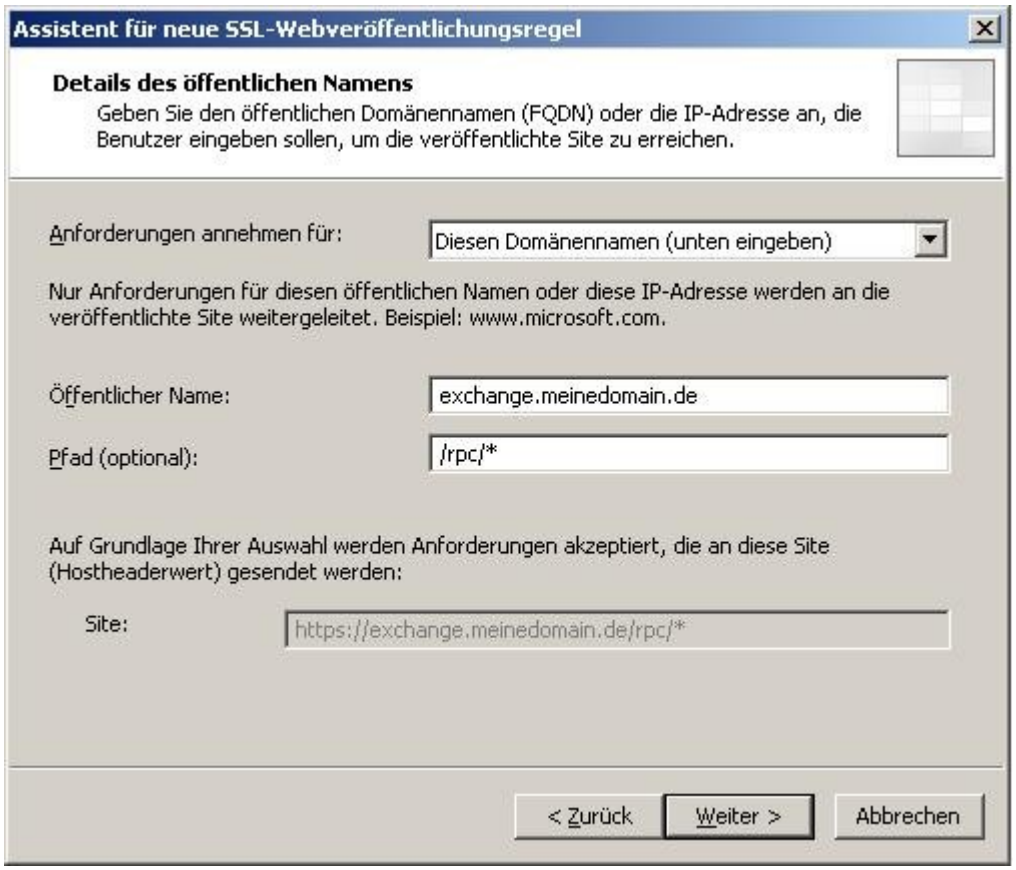
Als Regelaktion wählen Sie Zulassen aus.

Als Bridgingmodus wählen Sie sie die Option *Sichere Verbindung mit Clients und Webserver* aus, um einen SSL Tunnel zwischen Client und dem ISA Server und zwischem dem ISA Server und dem Exchange Server herzustellen.



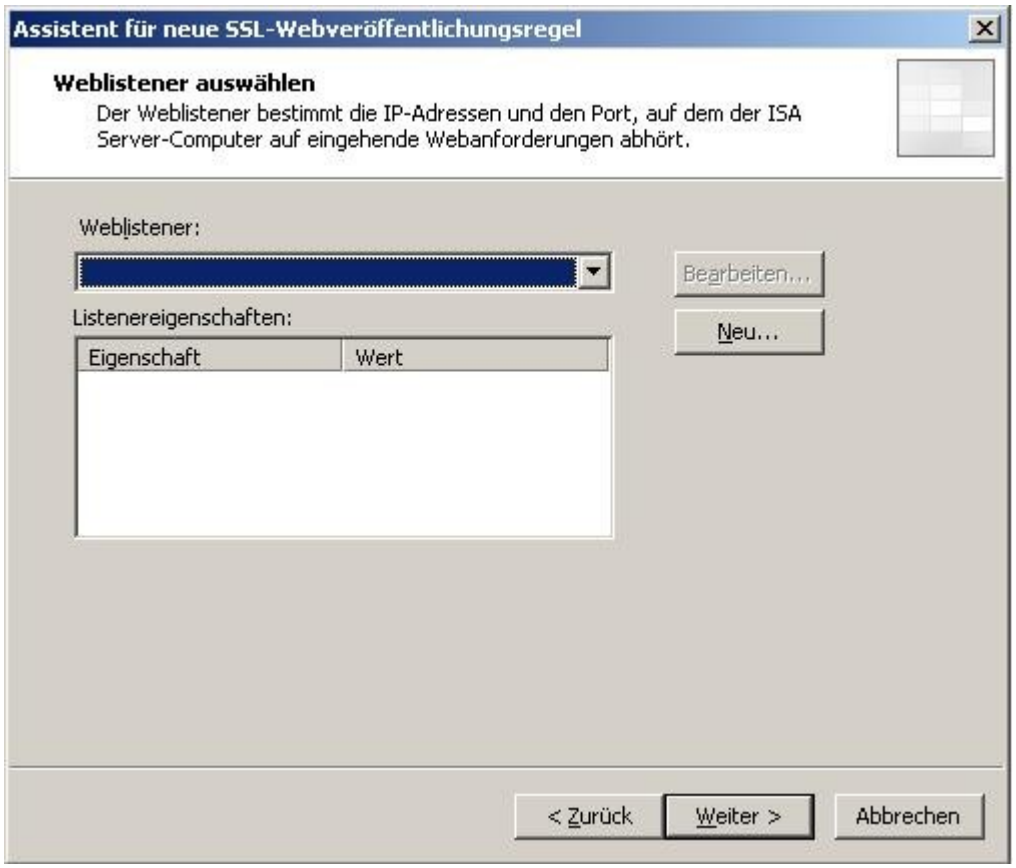
Geben Sie als Ziel der Firewallregel den Namen des internen Exchange Servers und als Pfad /RPC/* an.

Hinweis: Der Name des Zielservers muss mit dem FQDN des Zertifikates auf dem Exchange Server übereinstimmen. Sollte dies nicht der Fall sein, muss ein entsprechender Eintrag in der Hosts Datei auf dem ISA Server vorgenommen werden.



Sie müssen angeben unter welcher URL ihr Exchange Server von Extern zu erreichen ist. Der Pfad wird automatisch übernommen.

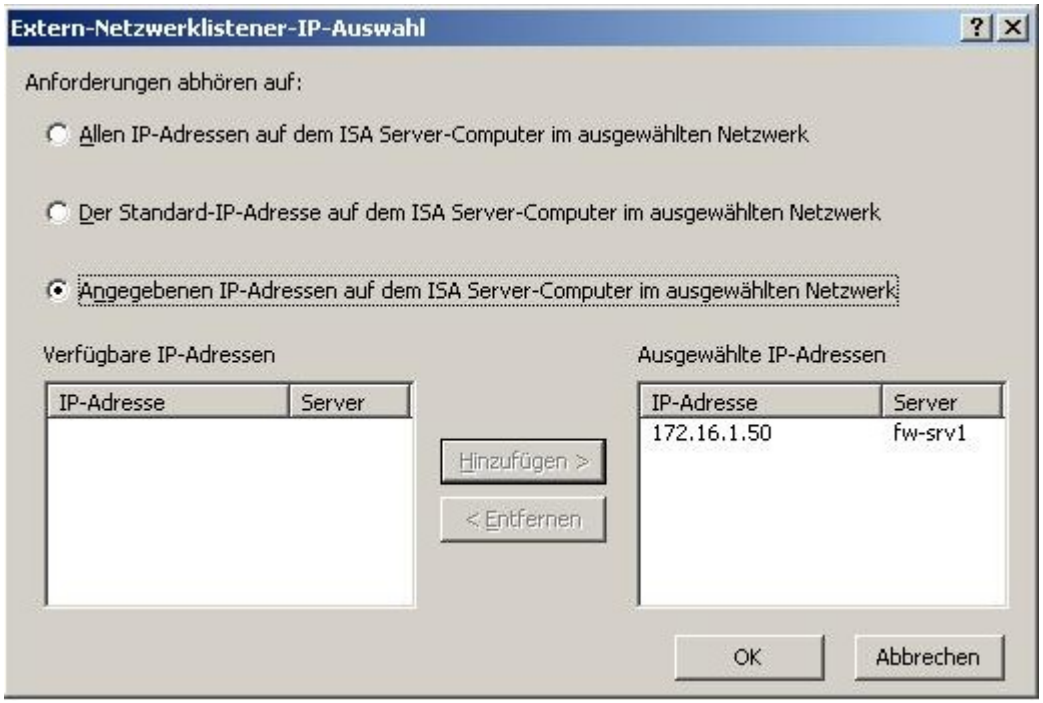
3.2 Erstellung/Konfiguration eines Weblisteners



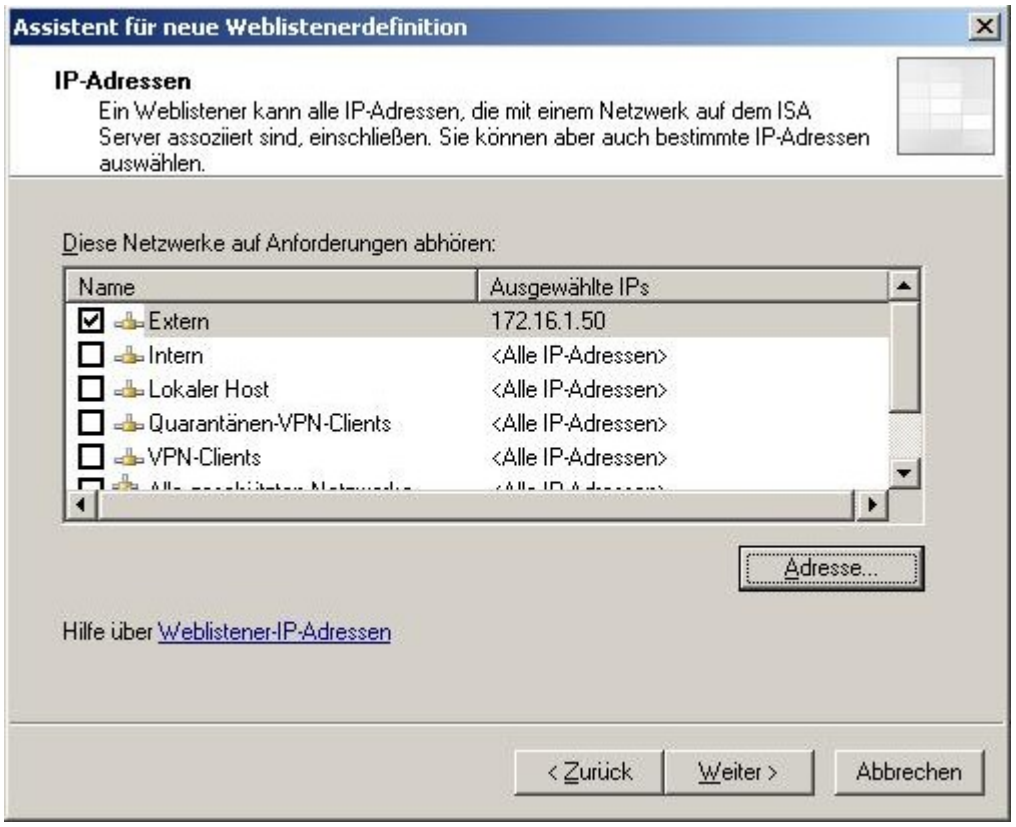
Erstellen Sie über den Button Neu einen neuen Weblistener

Vergeben Sie einen Namen im Assistenten zur Erstellung eines neuen Weblisteners.

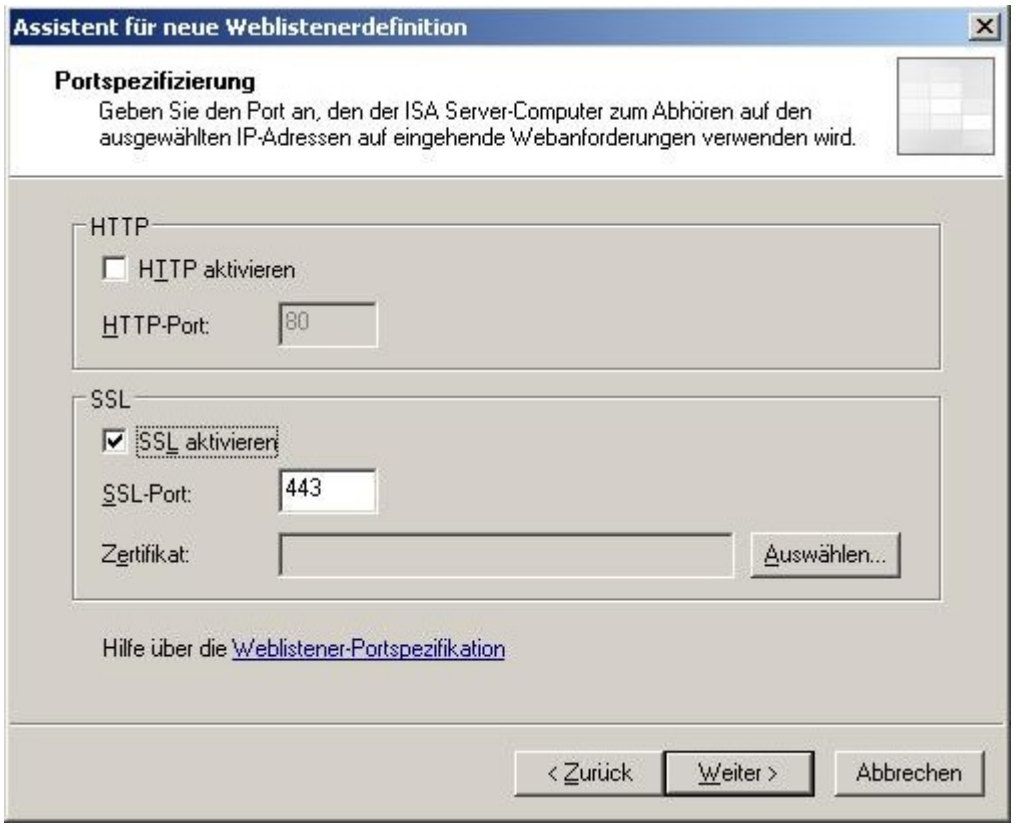
Geben Sie das Netzwerk an, von dem Zugriff zugelassen werden soll.



Wählen Sie die Option *Angegebenen IP-Adressen auf dem ISA Server-Computer im ausgewählten Netzwerk* aus, damit Sie die Möglichkeit haben eventuelle weitere Weblistener individuell zu konfigurieren. Fügen Sie die IP Adresse, auf der die Anfragen entgegengenommen werden sollen, hinzu.

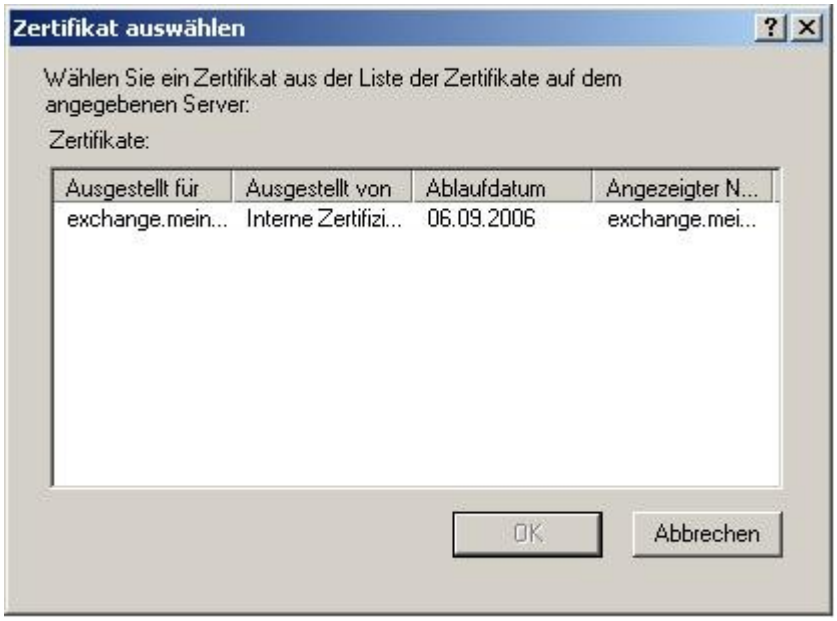


Unter dem ausgewählten Netzwerk sollte anschließend nur die angegebene IP Adresse ausgewählt sein.

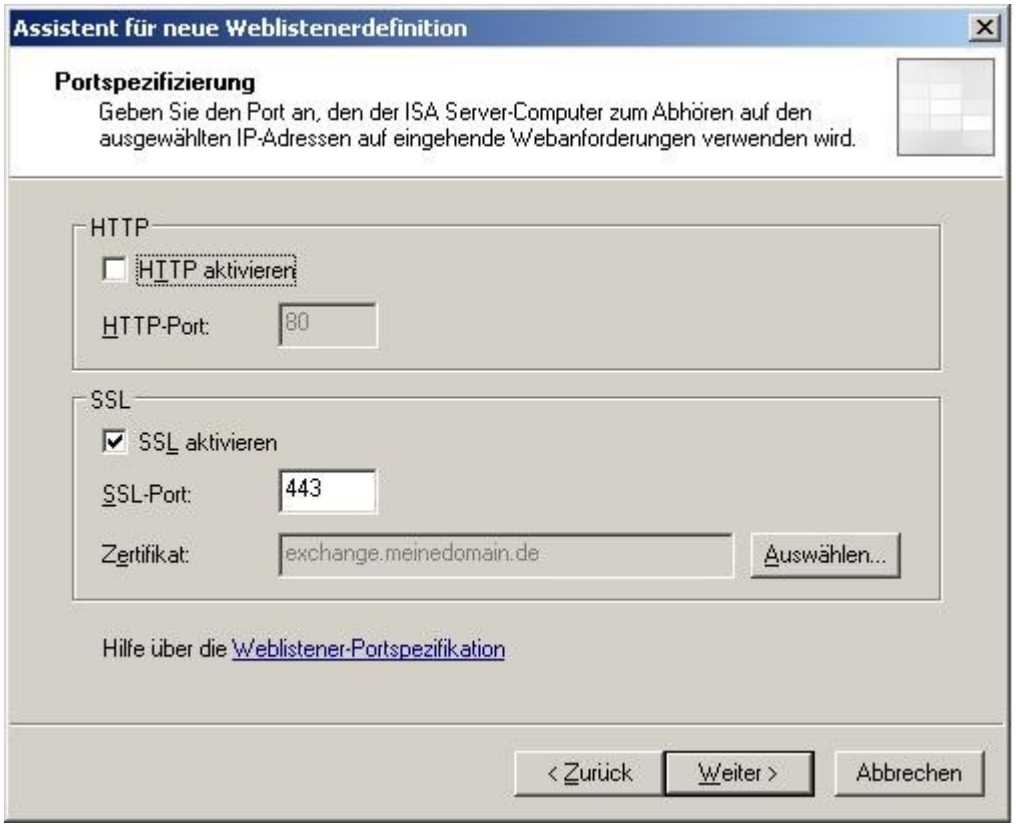


Deaktivieren Sie das Protokoll HTTP und aktivieren Sie das Protokoll SSL, um Anfragen nur über einen SSL Tunnel zu zulassen. Geben Sie über den Button Auswählen das Zertifikat für

die SSL Verschlüsselung an.



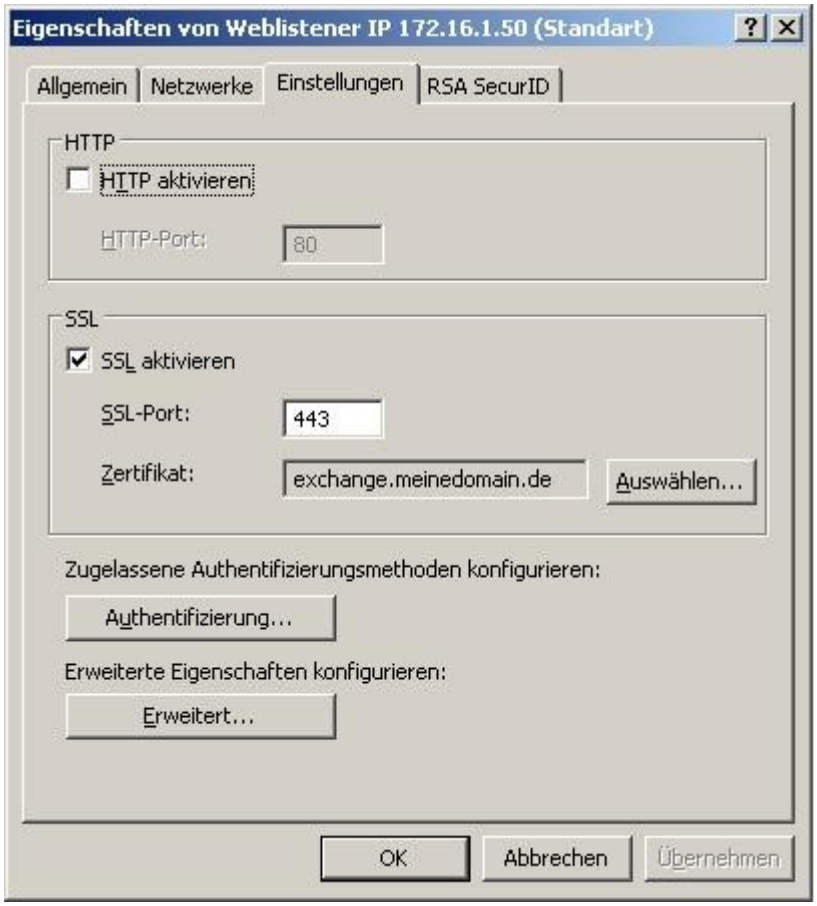
Wählen Sie das Zertifikat aus.



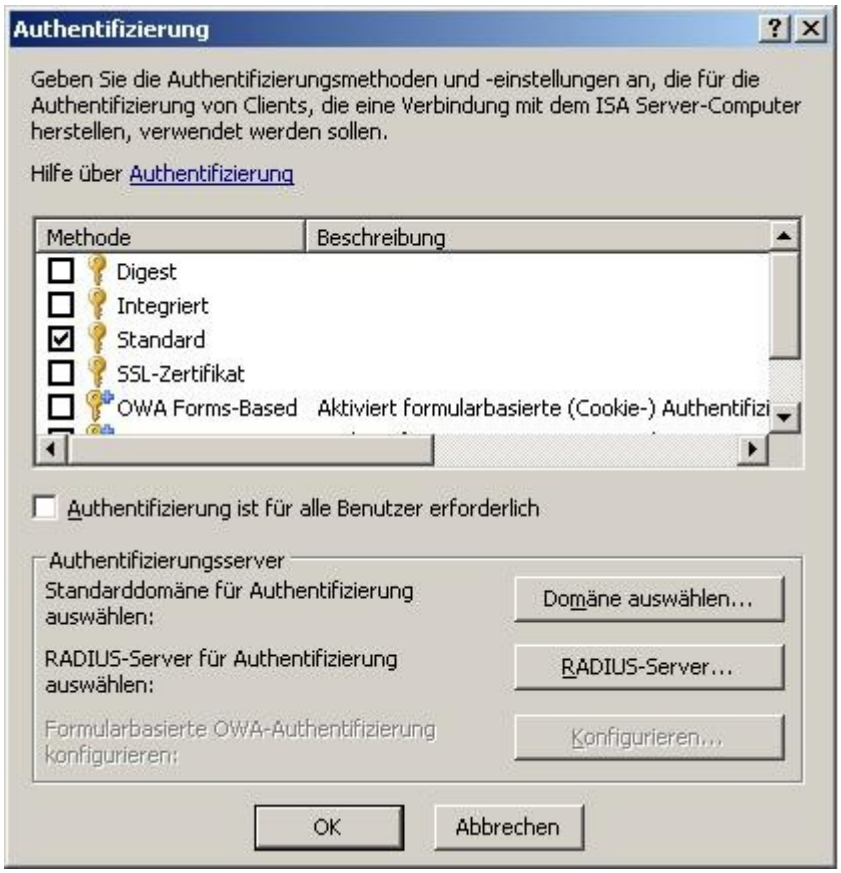
Anschließend sollte der Weblistener wie im Bild abgebildet konfiguriert sein.

Zum Abschluss bekommen Sie eine Zusammenfassung des Weblisteners angezeigt.

Ändern Sie die Authentifizierungsmethode über den Button Bearbeiten.

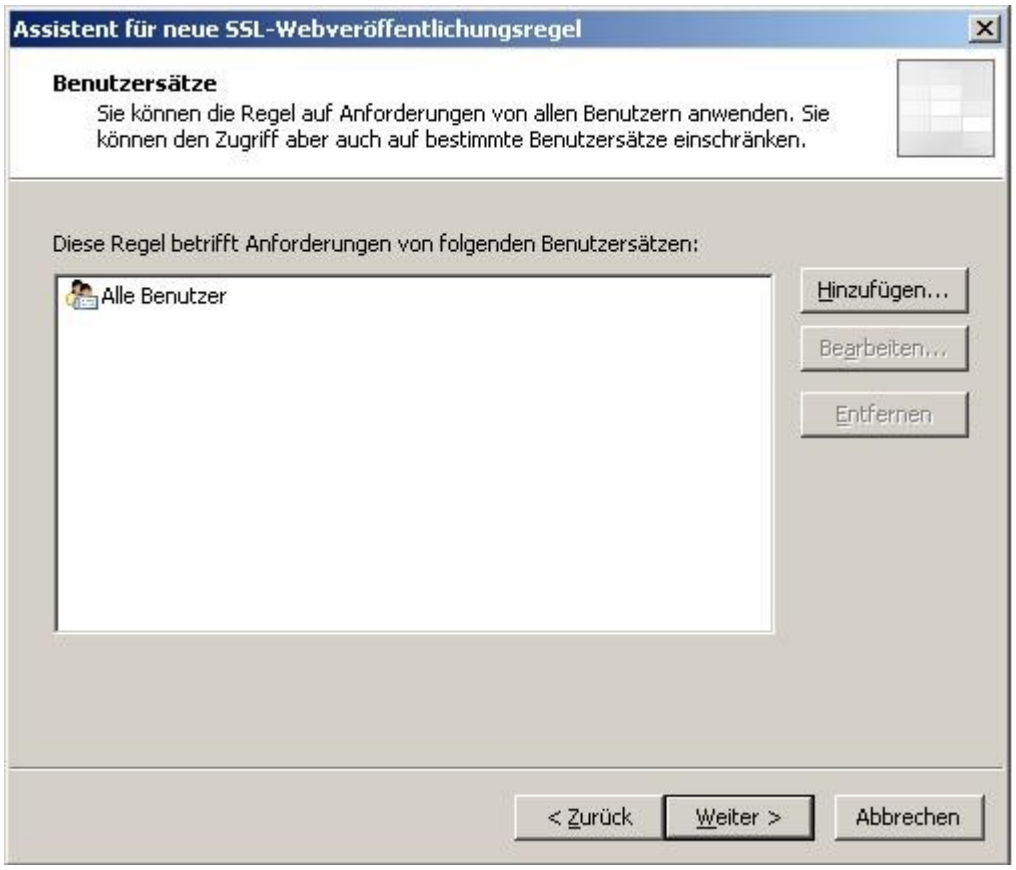


Öffnen Sie die Konfiguration der Authentifizierungsmethoden über Authentifizierung.



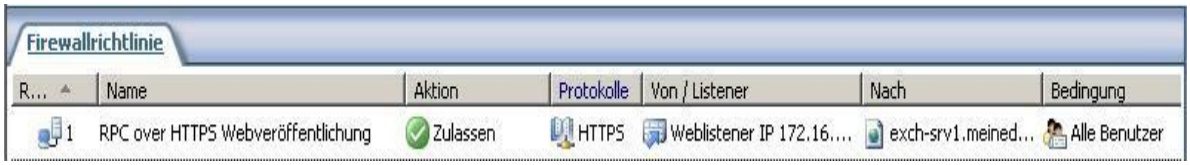
Wählen Sie als Authentifizierungsmethode nur Standart aus. Sie bekommen eine Sicherheitswarnung angezeigt, die Sie bestätigen. Ein Sicherheitsrisiko besteht hier nicht, da die Daten in einem SSL Tunnel übertragen werden.

3.3 Erstellen einer Sicheren Webserververöffentlichung (Teil 2)

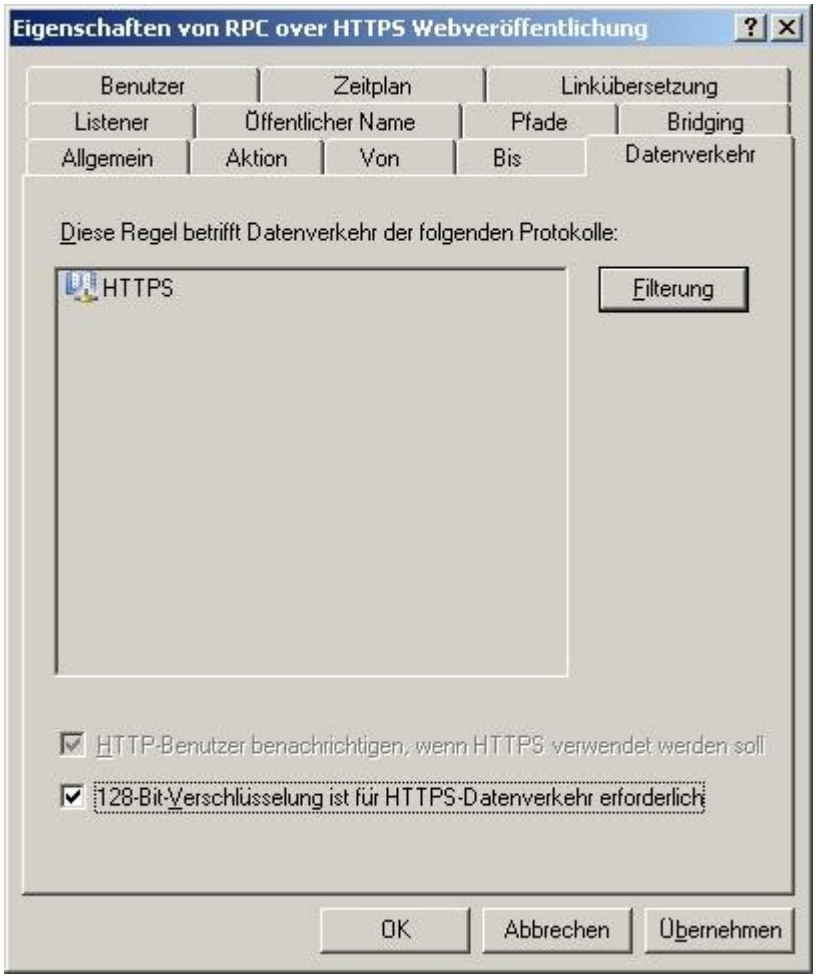


Hier könnten Sie den Zugriff auf eine bestimmte Benutzergruppe einschränken.

Zum Abschluss bekommen Sie eine Zusammenfassung der Firewallregel angezeigt.

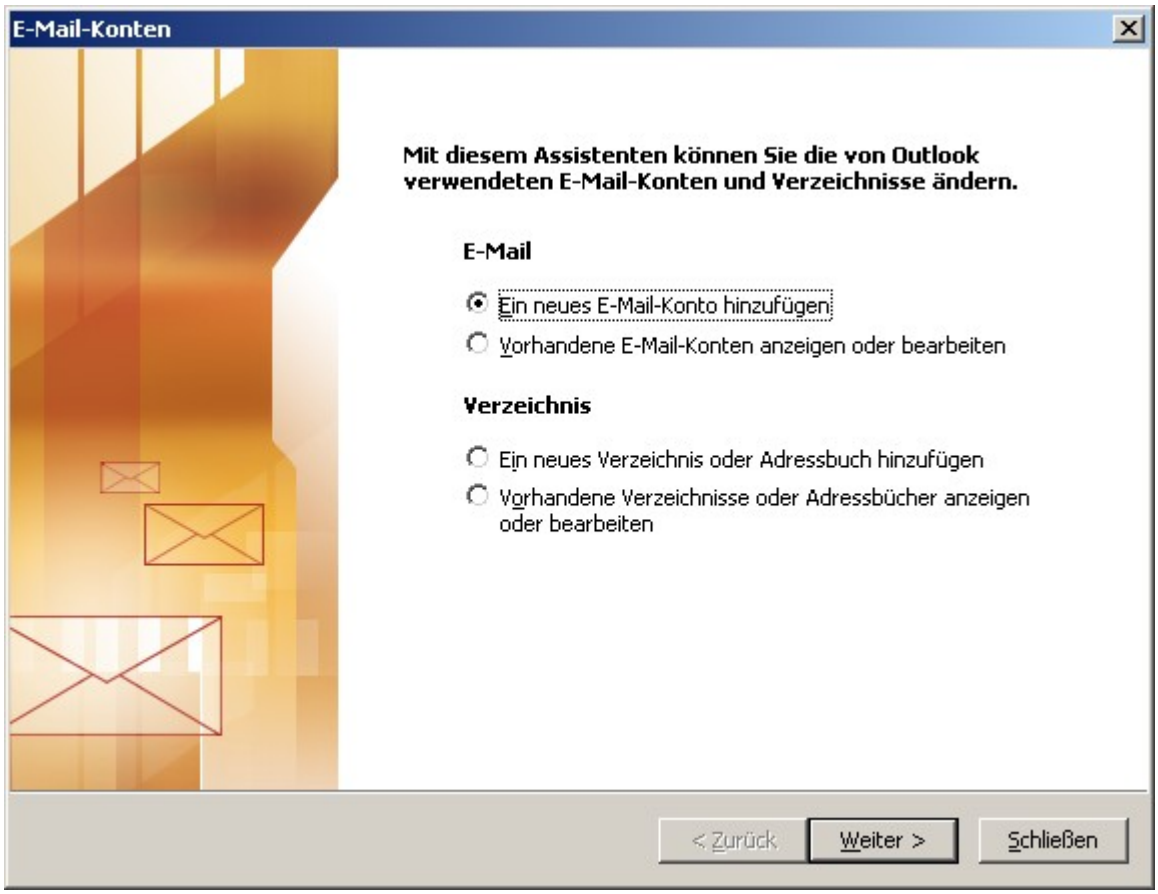


Öffnen Sie zur weitern Konfiguration die Eigenschaften der Veröffentlichungsregel.

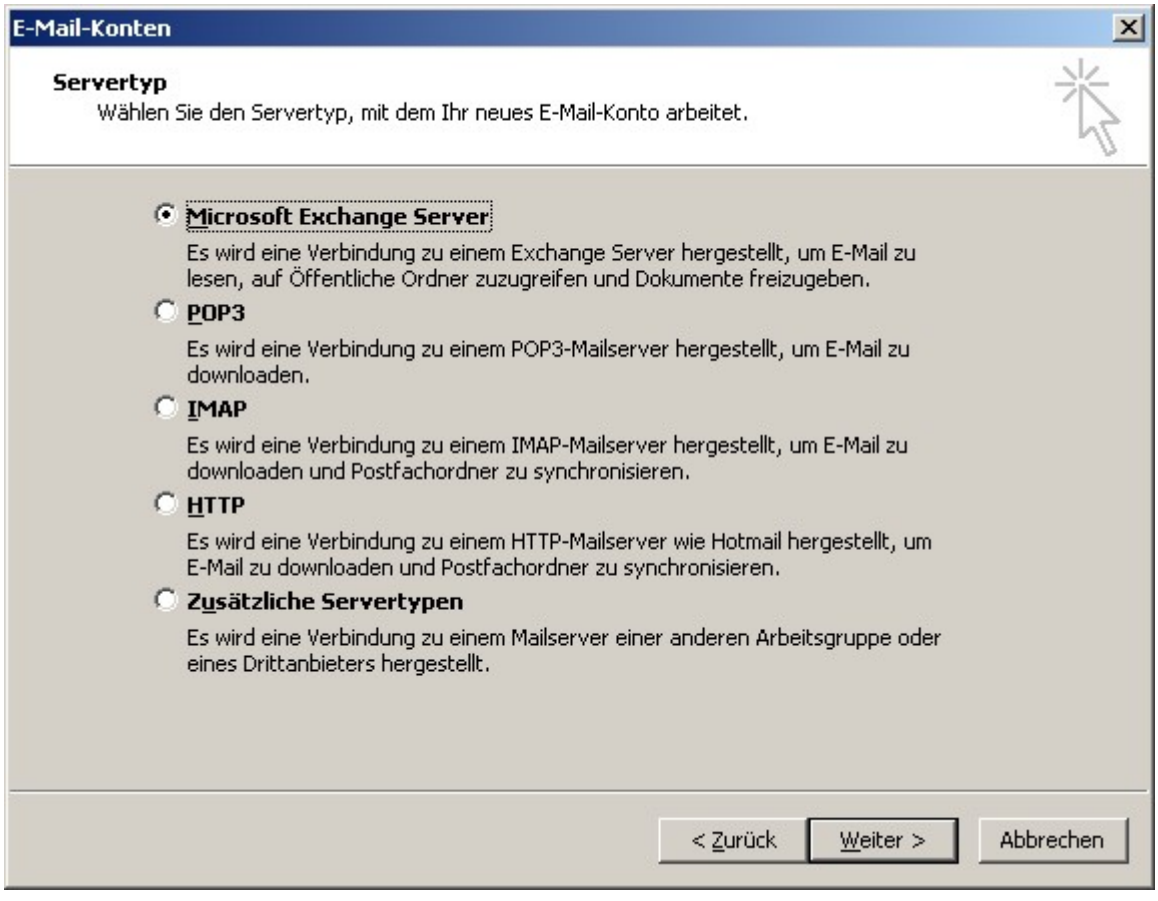


Unter dem Karteireiter Allgemein können Sie eine Verschlüsselungsstärke von 128 Bit fordern.

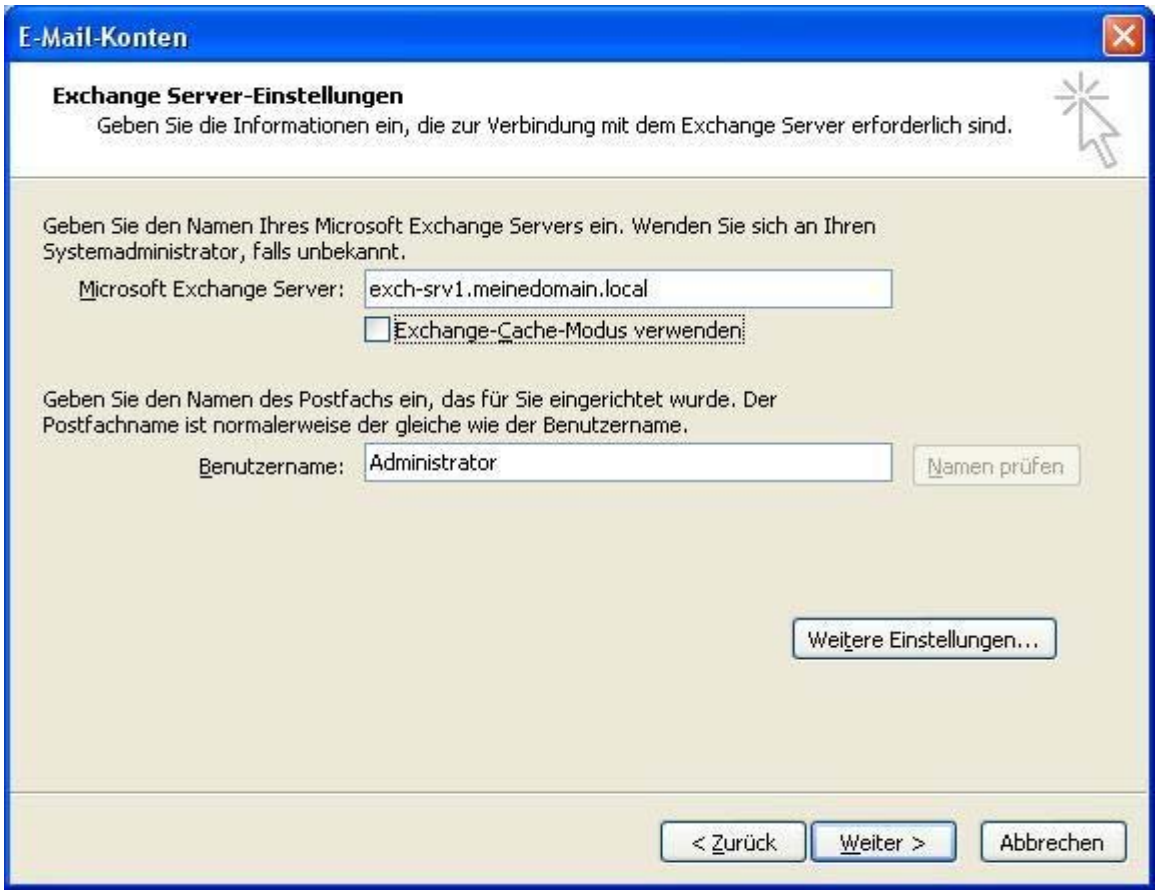
4. Konfiguration von Outlook 2003



Erstellen Sie für Outlook ein Profil und fügen diesem ein neues Konto hinzu.

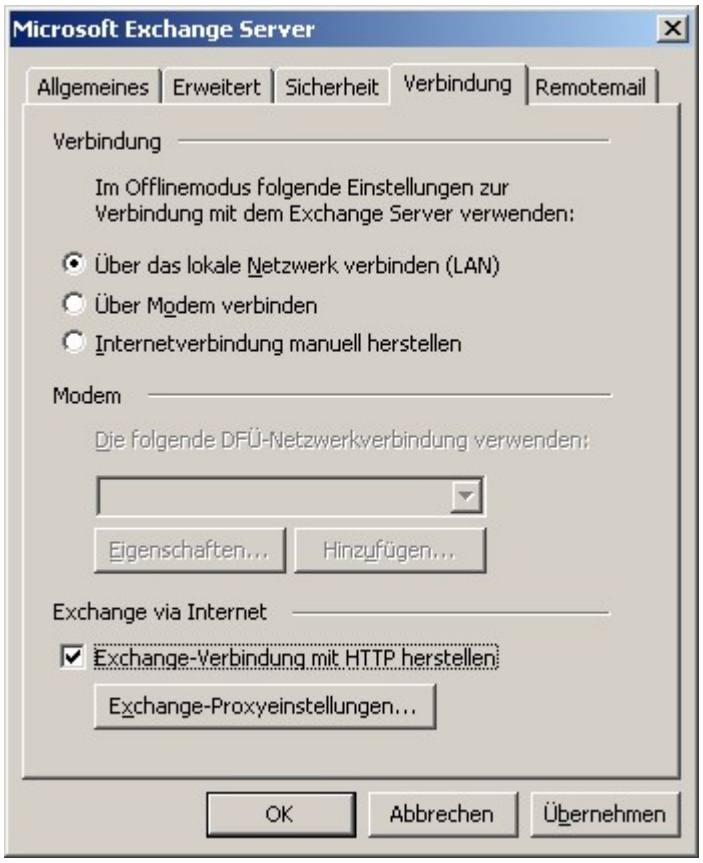


Als Serverart wählen Sie hier Microsoft Exchange Server aus.

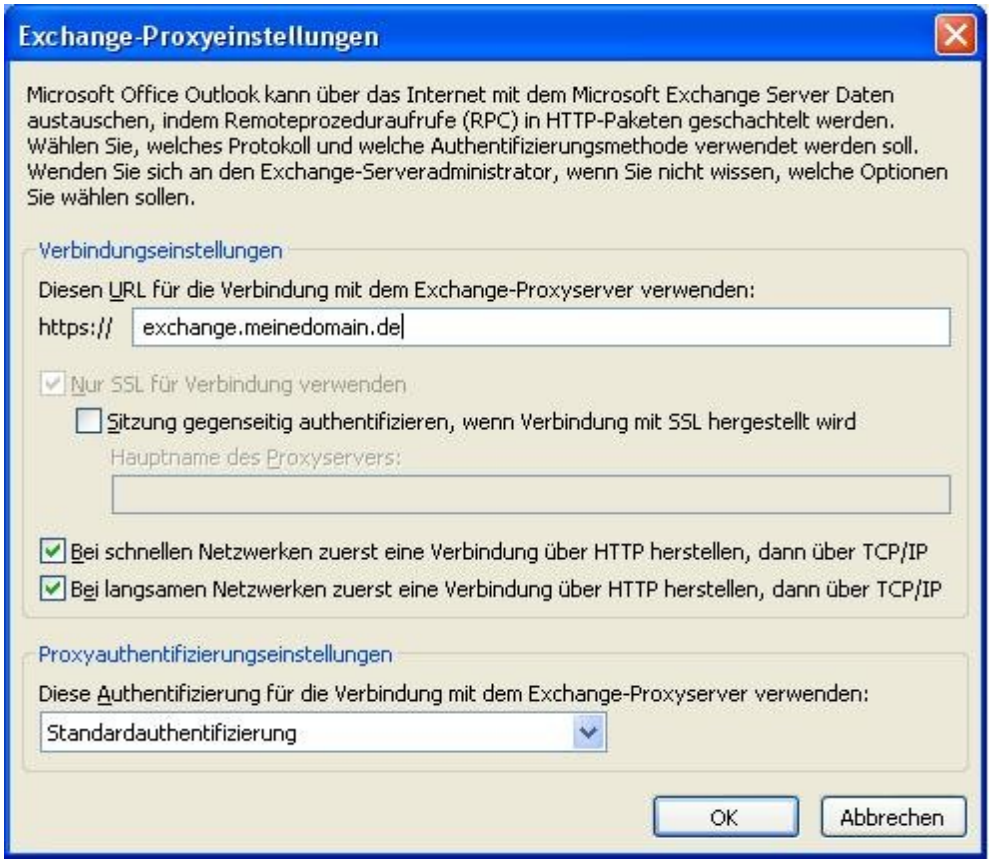


Tragen Sie unter Microsoft Exchange Server den **internen** Servernamen des Exchange Servers ein.
Als Benutzername tragen Sie das entsprechende Postfach ein und öffnen anschließend die weiteren Einstellungen.

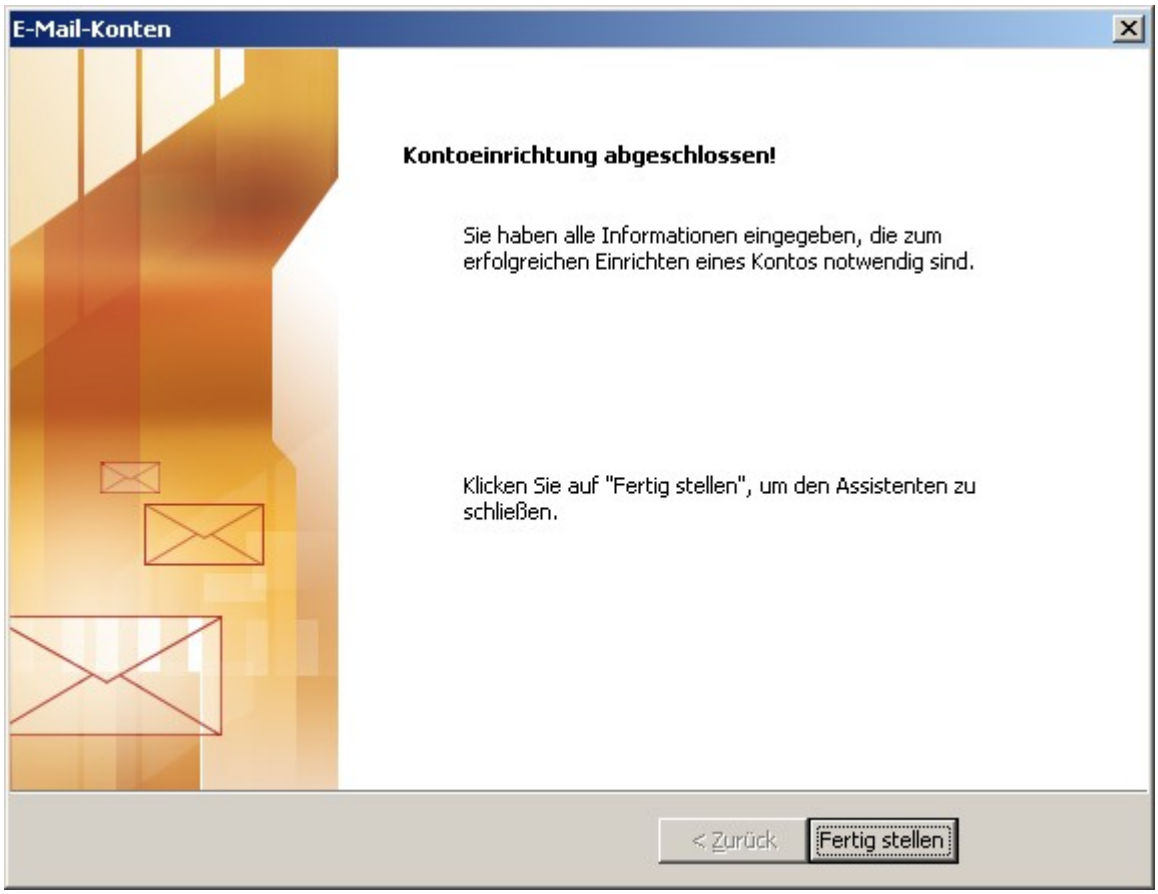
Hinweis: Bei sehr großen Postfächern empfiehlt es sich, den Cachemodus zum Verbindungstest zu deaktivieren. Dieser sollte allerdings aus Performancegründen nach erfolgreicher Verbindung über das Menü Extras -> Konten wieder aktiviert werden.



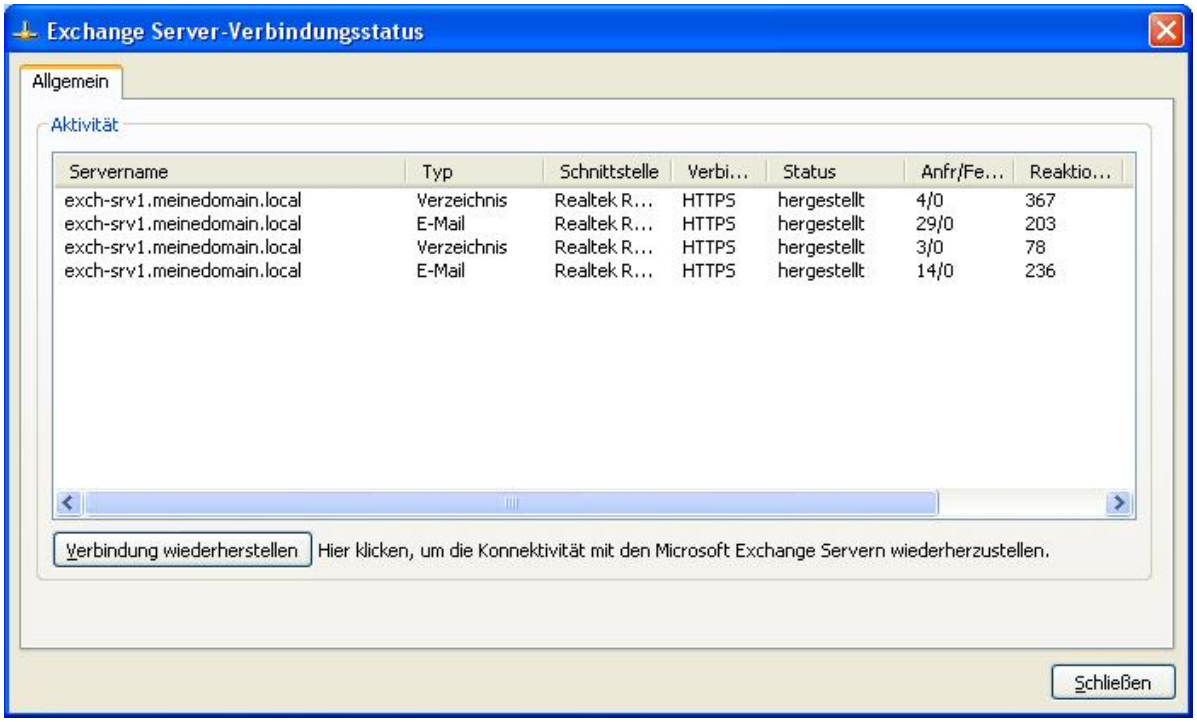
Setzen Sie den Haken bei Exchange Verbindung mit HTTP herstellen unter dem Karteireiter Verbindung. Weitere Einstellungen müssen unter dem Punkt Exchange Proxyeinstellungen vorgenommen werden.



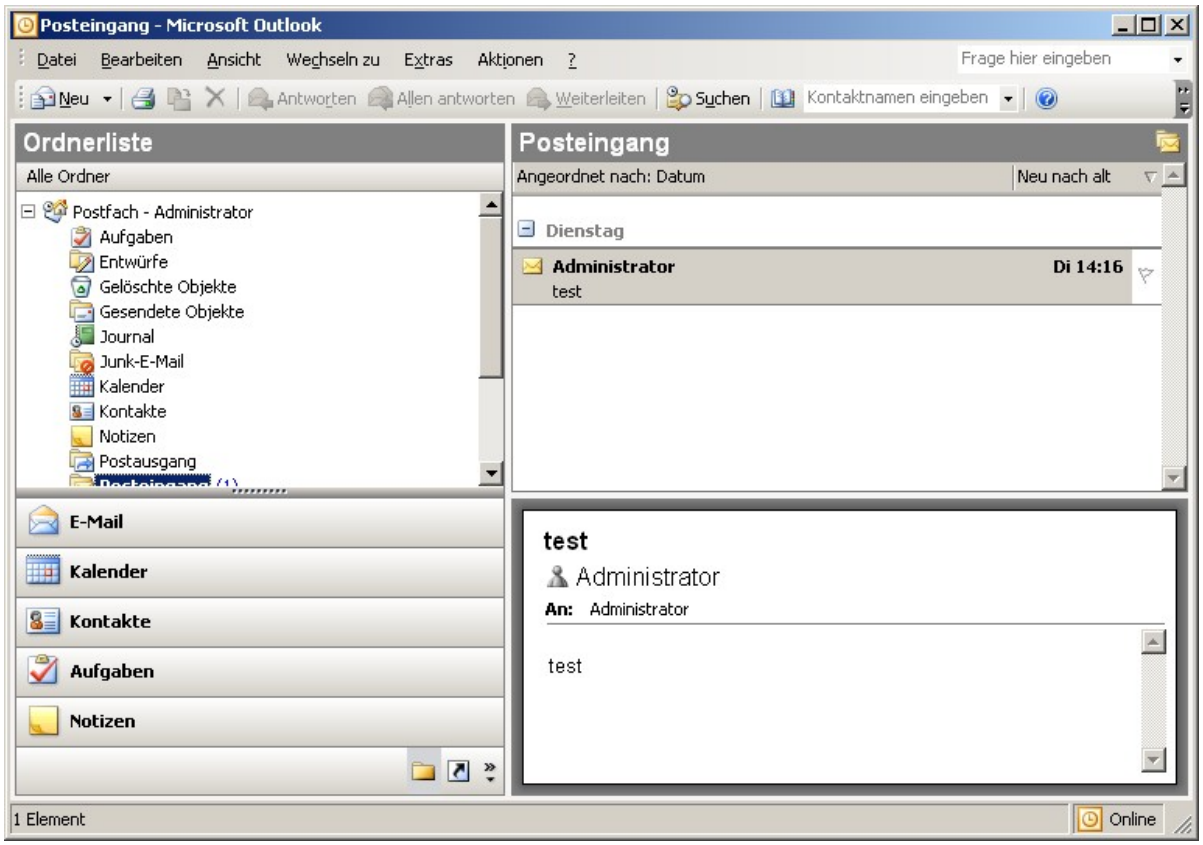
Als Verbindungs-URL tragen Sie hier die externe URL ein unter der Sie die Veröffentlichung erstellt haben. Setzen Sie die beiden Haken für die HTTP Verbindung und stellen Sie die Authentifizierungsmehtode auf Standartauthentifizierung um.



Durch Schließen der vorigen Fenster ist die Konfiguration abgeschlossen.



Öffnen Sie anschließend Outlook 2003 über Start -> Ausführen mit dem Befehl Outlook /RPCDIAG. Es sollte obiges Fenster erscheinen in dem Sie sehen können, dass die Verbindung über HTTPS hergestellt wird.



Bei erfolgreicher Verbindung können Sie nun Outlook 2003 mit allen Features von Extern über einen SSL Tunnel verwenden.

5. Fehlerbehandlung

Sollte es nicht zum Verbindungsaufbau kommen, überprüfen Sie bitte folgende Schritte:

5.1 Überprüfung des internen SSL Tunnels

Öffnen Sie hierzu auf dem ISA Server ein Browserfenster und geben die interne URL des Exchange Servers und als Pfad /rpc/, hier exch-srv1.meinedomain.local/rpc/. Wenn alles funktioniert sollten Sie ein Anmeldefenster angezeigt bekommen, in das Sie die Anmeldedaten des Benutzers, in der Form Domäne\Benutzer, eingeben. Danach sollte eine HTTP 403.2 Fehlermeldung angezeigt werden. Sollten Sie eine Zertifikatswarnung angezeigt bekommen, beheben Sie die angezeigten Fehler.

Wichtig auf dem ISA Server ist, dass sich das Zertifizierungsstellenzertifikat im Container für Vertrauenswürdige Stammzeritifzierungsstellen des Computers befindet.

5.2 Überprüfung des externen SSL Tunnels

Öffnen Sie hierzu auf dem externen Client ein Browserfenster und geben die externe URL des Exchange Servers und als Pfad /rpc/, hier exchange.meinedomain.de/rpc/. Wenn alles funktioniert sollten Sie ein Anmeldefenster angezeigt bekommen, in das Sie die Anmeldedaten des Benutzers, in der Form Domäne\Benutzer, eingeben. Danach sollte eine HTTP 403.2 Fehlermeldung angezeigt werden. Sollten Sie eine Zertifikatswarnung angezeigt bekommen, beheben Sie die angezeigten Fehler.

Zeitabgleich mit einem externen Zeitserver

Die Informationen in diesem Artikel beziehen sich auf:

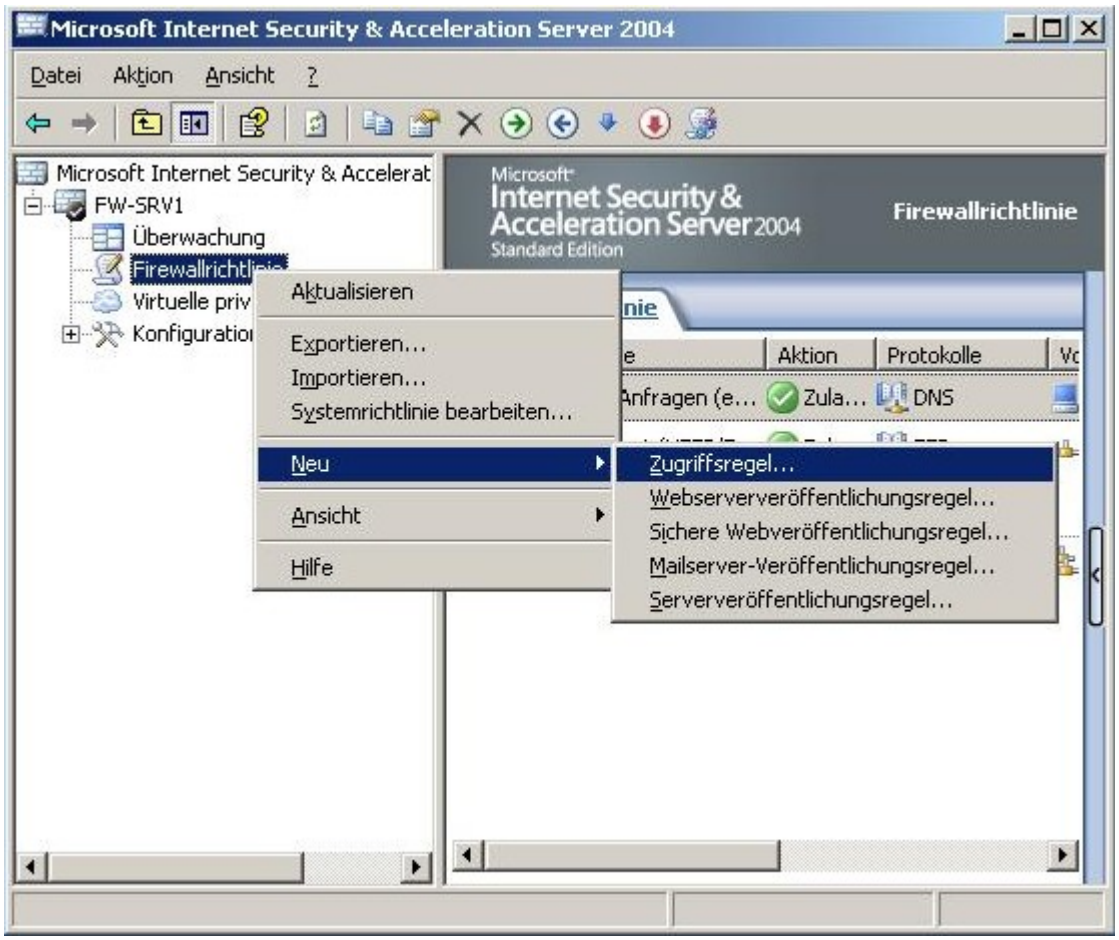
- Microsoft ISA Server 2004
- Microsoft Windows Server 2000
- Microsoft Windows Server 2003

Die richtige Uhrzeit in einem Netzwerk ist eine wichtige Sache, die von sehr vielen Administratoren
vernachlässigt wird. Aufgrund einer falschen Uhrzeit kann es vorkommen, dass eine Verbindung verweigert
wird, ein wichtiger Aspekt ist dies z.B. bei Verschlüsselung, oder es entstehen Falschbuchungen in einem
Warenwirtschaftssystem.

Erkennen, ob ein Zeitserver auf einem Server konfiguriert ist, können Sie durch Fehlermeldungen vom
Typ W32Time im Ereignissprotokoll.

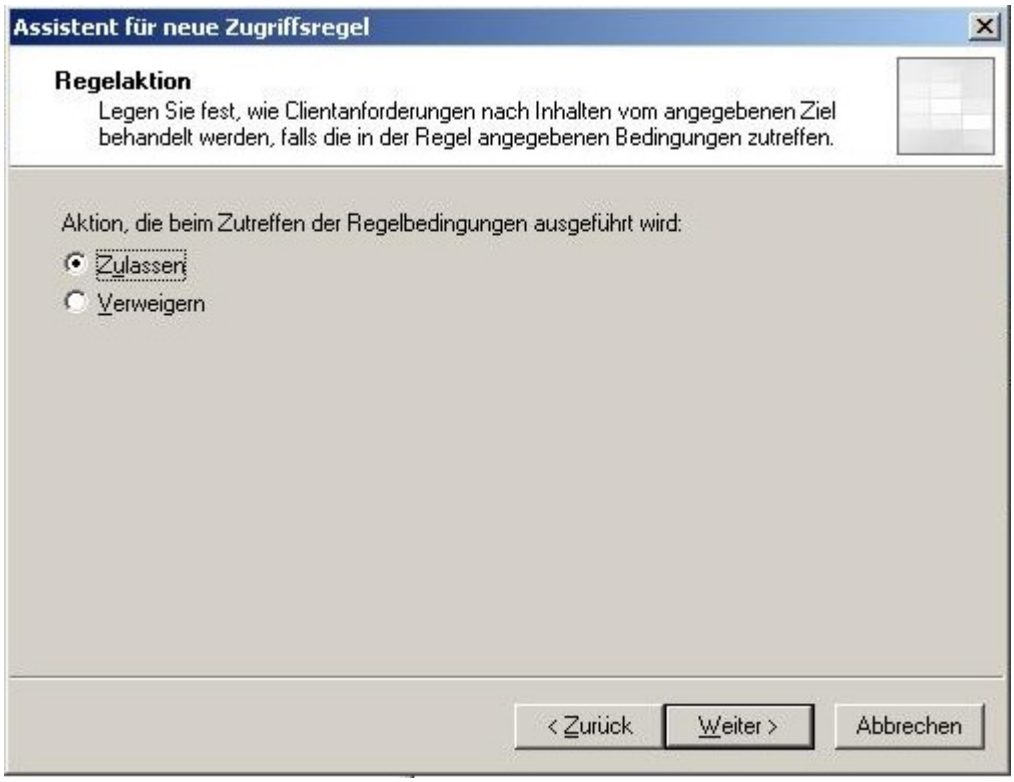
Wie Sie einen Server, in Verbindung mit dem ISA 2004, für die Verwendung eines Zeitservers konfigurieren
wird in dieser Anleitung erklärt.

1. Erstellen einer Firewallrichtlinie

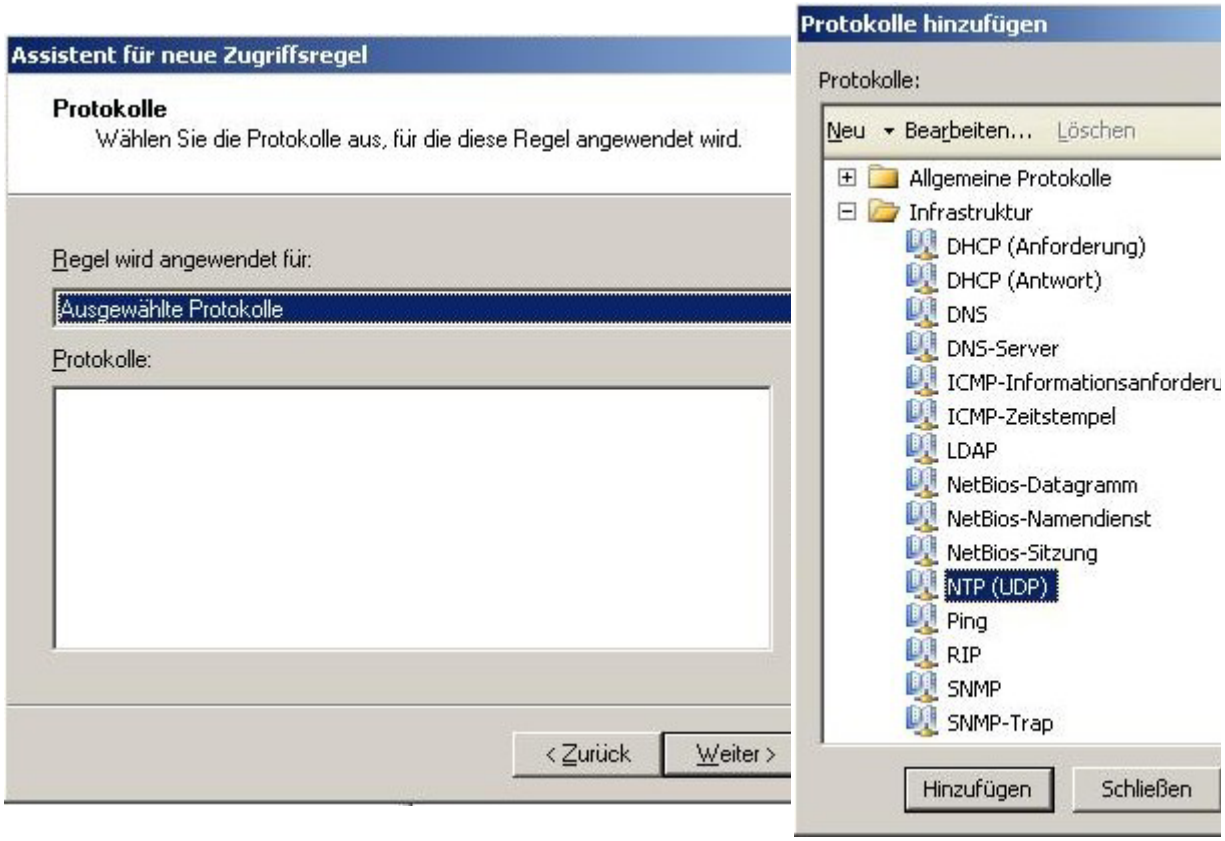


Erstellen Sie eine neue Firewallrichtlinie über Neu->Zugriffsregel.

Vergeben Sie der Regel einen aussagekräftigen Namen.

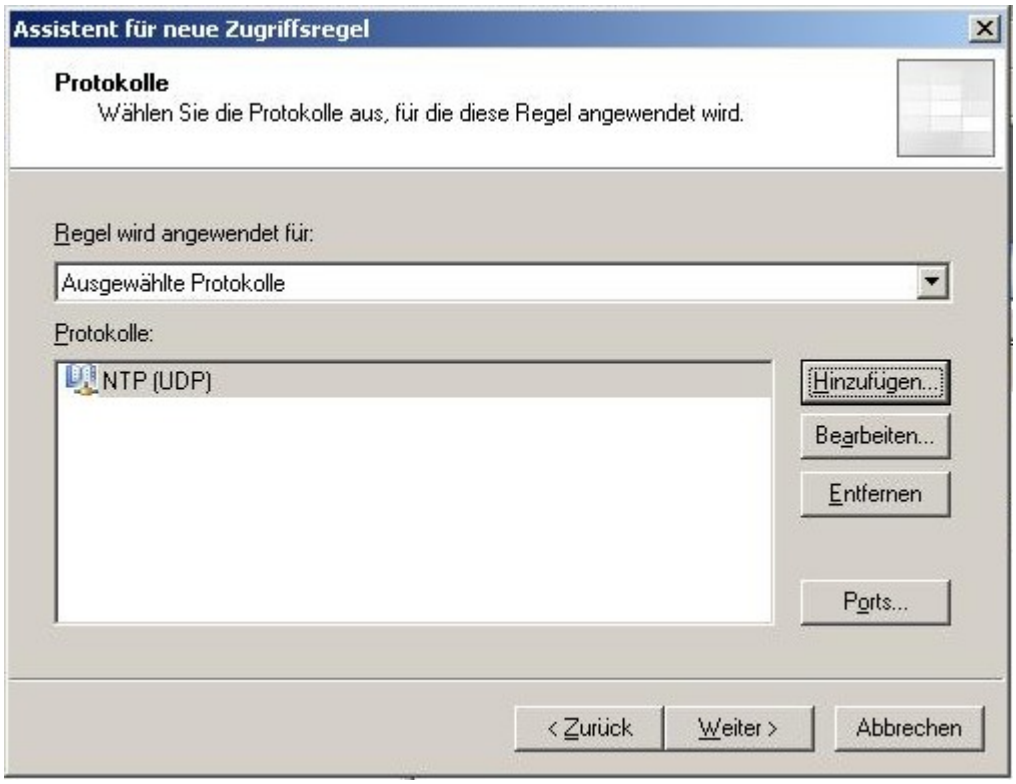


Wählen Sie die Option Zulassen aus.



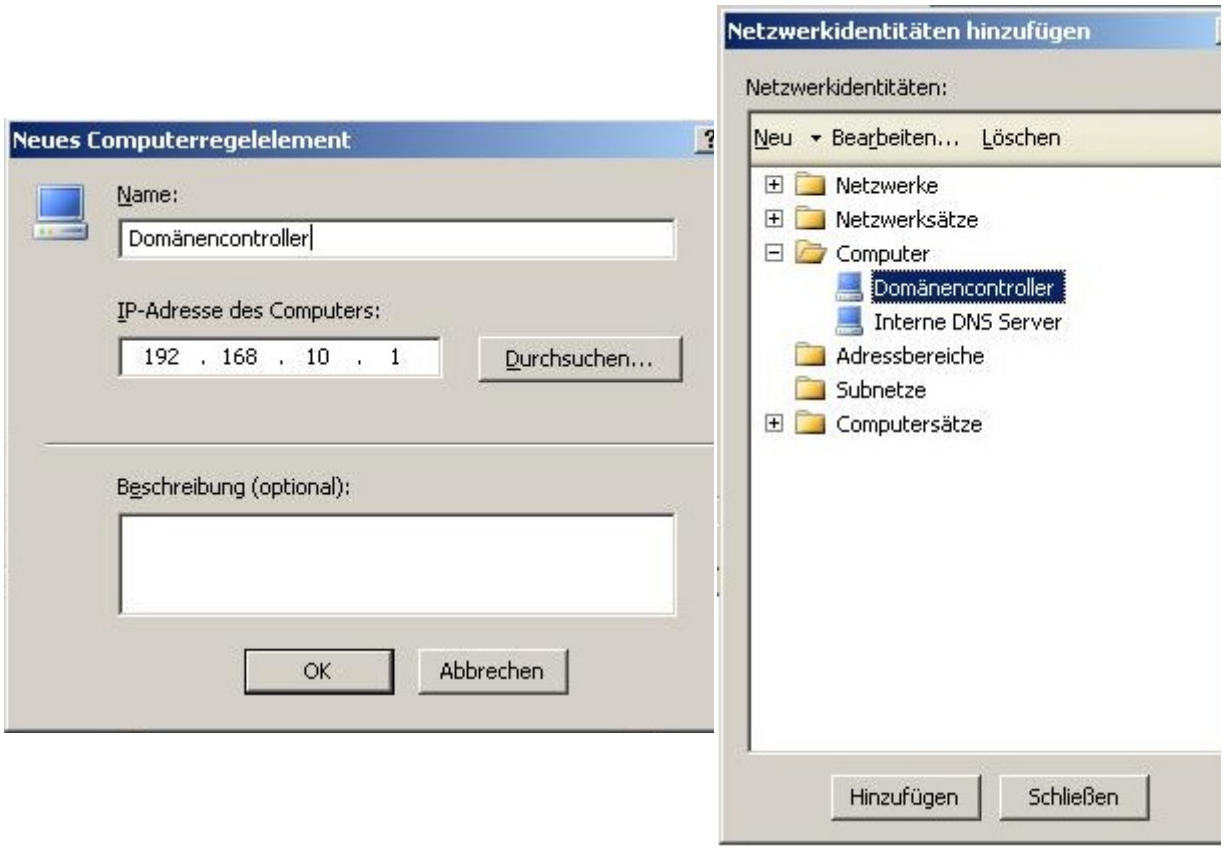
Ändern Sie unter *Regel wird angewendet für* die Auswahl auf Ausgewählte Protokolle ab und fügen
das unter der Kategorie Infrastruktor befindliche Protokoll NTP(UDP) hinzu, das für den

Zeitabgleich
einem externen Zeitserver benötigt wird.



Anschließend solte nur das Protokoll NTP(UDP) ausgewählt sein.

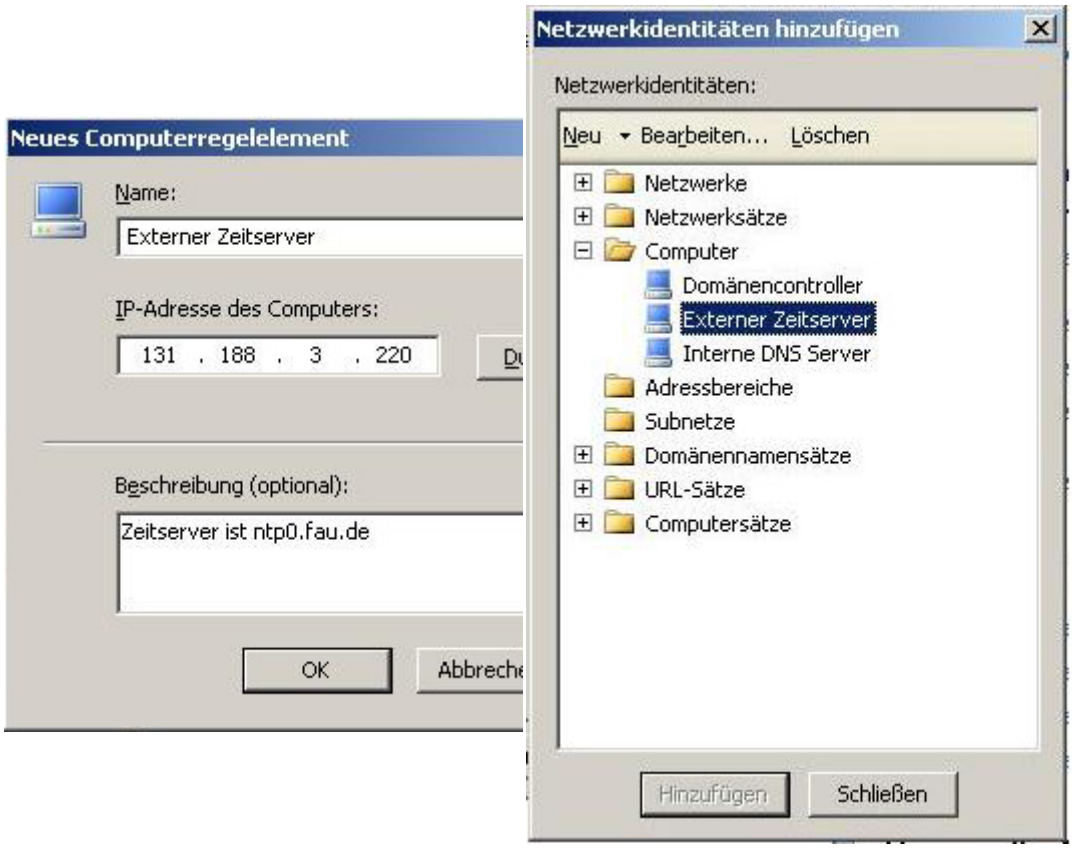
Es muss angegeben werden, aus welchem Netz bzw. von welchem Objekt die Anfragen zugelassen werden.
In dieser Anleitung wird der Zugriff auf einen einzelnen internen Server beschränkt, was aus Sicher-
heitsgründen zu empfehlen ist. Erstellen Sie ein neues Computerregelelement über Neu->Computer.



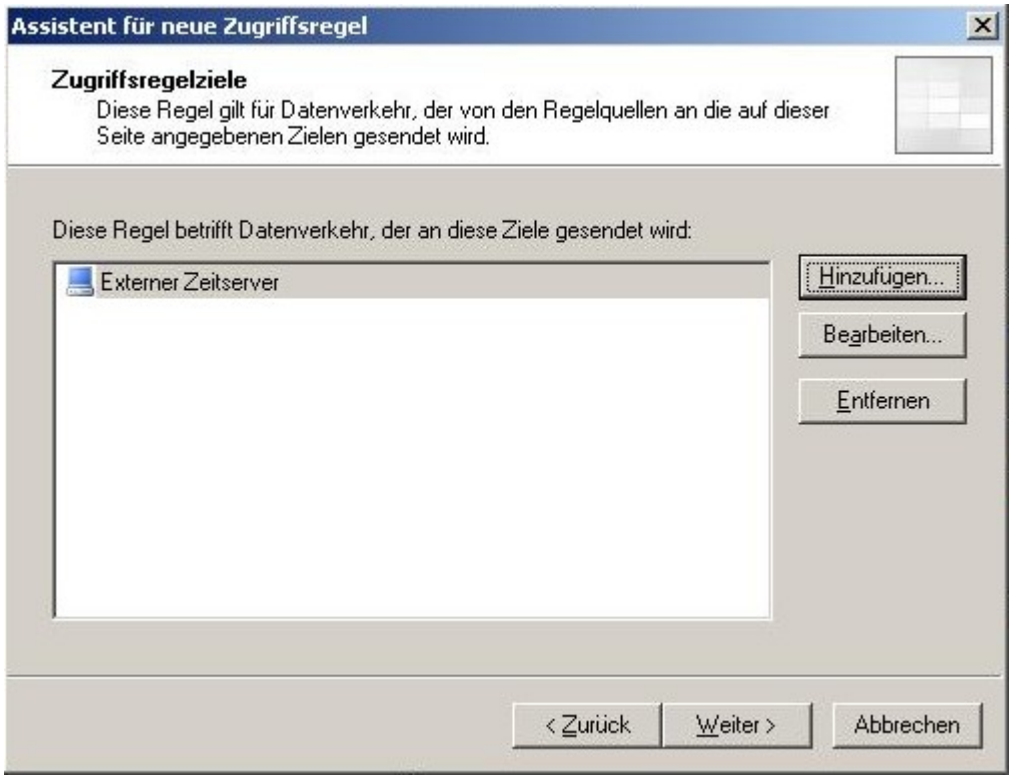
Vergeben Sie dem Computerregelelement einen Namen und geben Sie die IP Adresse des Servers an.
Optional kann eine Beschreibung angegeben werden. Fügen Sie das gerade erstellte Computerregel-
element hinzu, damit Anfragen nur von diesem Server erlaubt sind.

Als Quelle sollte nur der ausgewählte Server stehen.

Anschließend müssen Sie angeben in welches Netz bzw. an welches Objekt Zeitanfragen gesendet
werden dürfen. Erstellen Sie hierzu ein neues Computerregelelement über Neu->Computer.



Vergeben Sie einen Namen und tragen Sie die IP Adresse des externen Zeitservers ein. Über Durchsuchen können Sie den FQDN des Zeitservers angeben, der darauf in eine IP Adresse umgewandelt wird. Optional kann hier eine Beschreibung angegeben werden. Fügen Sie der Regel das gerade erstellte Computerregelelement hinzu.



Als Ziel sollte nur der ausgewählte Server stehen.

Belassen Sie die Einstellung Alle Benutzer, da der Zeitabgleich über einen Dienst gesteuert wird. Der Zugriff wurde in vorigen Schritten nur auf einen Server beschränkt, somit ist dies kein Sicherheitsrisiko.

Abschließend bekommen Sie eine Zusammenfassung der Firewallregel angezeigt.

2. Konfigurieren des Servers für einen externen Zeitserver

Damit der Zeitabgleich funktioniert muss der Server für einen externen Zeitserver konfiguriert werden.

2.1 Windows 2000 Server

Öffnen Sie über Start->Ausführen->cmd ein Eingabeaufforderungsfenster

Mit dem Befehl **net time /setsntp:ntp0.fau.de** legen Sie den externen Zeitserver fest. ntp0.fau.de ist in dieser Anleitung der externe Zeitserver. Einen Link zu externen Zeitservern finden Sie am Ende dieser Anleitung.

Testen können Sie die Konfiguration, indem Sie folgende Befehle eingeben:

Beenden Sie zunächst den Zeitdienst über den Befehl: **net stop w32time** .
Zur einmaligen manuellen Syncronisation geben Sie folgendes ein: **w32tm -once**
Danach starten Sie den Zeitdienst wieder über: **net start w32time**

2.2 Windows 2003 Server

Bei einem Windows 2003 Server ist die Konfiguration des externen zeitservers ähnlich. Öffen Sie auch hier ein
Eingabeaufforderungsfenster über Start-Ausführen->cmd .

Legen Sie den externen Zeitserver über den Befehl **net time /setsntp:ntp0.fau.de** fest. ntp0.fau.de ist in dieser Anleitung der externe Zeitserver. Einen Link zu externen Zeitservern finden Sie am Ende dieser Anleitung.

Ob der Abgleich mit dem Zeitserver funktioniert können Sie mit folgendem Befehl testen: **w32tm /resync**

3. Nützliche Links zum Thema Zeitsyncronisation

In folgendem Link finden Sie eine Liste von externen Zeitservern, die für den Zeitabgleich verwendet werden kann.
Bietet Ihr ISP auch diesen Dienst an, können Sie auch diesen Zeitserver verwenden.

Outlook Webaccess per SSL mit Formsbased Authentification mit dem ISA 2004

Die Informationen in diesem Artikel beziehen sich auf:

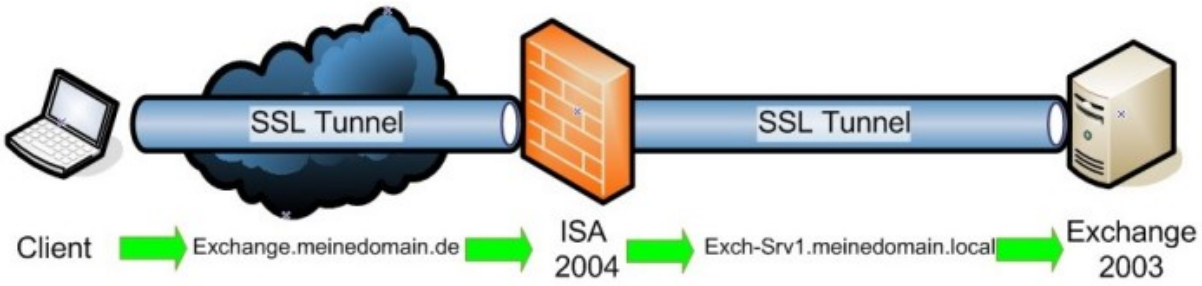
- Microsoft ISA Server 2004
- Microsoft Exchange Server 2003

Outlook Webaccess ermöglicht den Zugriff auf Ihr Postfach über einen Webbrowser. Durch eine SSL Verschlüsselung und das neue Feature im ISA 2004, der Formsbased Authentification, kann dieser Zugriff sicher eingerichtet werden. Die Authentifizierung erfolgt bei dieser Authentifizierungsmethode über ein Cookie, durch das überprüft wird, ob der Benutzer, nach erfolgreicher Anmeldung, authentifiziert ist. Das Cookie wird nicht auf dem Computer gespeichert, somit bietet diese Methode einen sicheren Zugang von öffentlichen Computern.

Vorteile dieser Verbindungsmethode sind:

- Es können für die unterschiedlichen Computertypen (Öffentlich/Privat) unterschiedliche Sicherheitseinstellunge bzgl. Timeout getroffen werden
- Es können für die unterschiedlichen Computertypen (Öffentlich/Privat) unterschiedliche Sicherheitseinstellunge bzgl. E-Mail Anlagen getroffen werden
- Das Cookie ist nur während dieser Sitzung gültig und verfällt beim Schließen des Browsers oder beim Wechsel der Seite
- Wenn das auch nicht wirklich ein Vorteil ist, aber die Anmeldung per OWA Formsbased Authentification ist Benutzerfreundlicher

Szenario



In dieser Anleitung wird die Verbindung zum Exchange Server mittels SSL Bridging hergestellt, d.h. es besteht ein SSL Tunnel zwischen dem Client und dem ISA Server und ein neuer Tunnel zwischen dem ISA- und dem Exchange Server. Hierzu sind zwei Webserverzertifikate für die SSL Verbindung notwendig. Ein Zertifikat für die Verbindung vom Client zum ISA Server für exchange.meinedomain.de, auf dem ISA Server, und intern

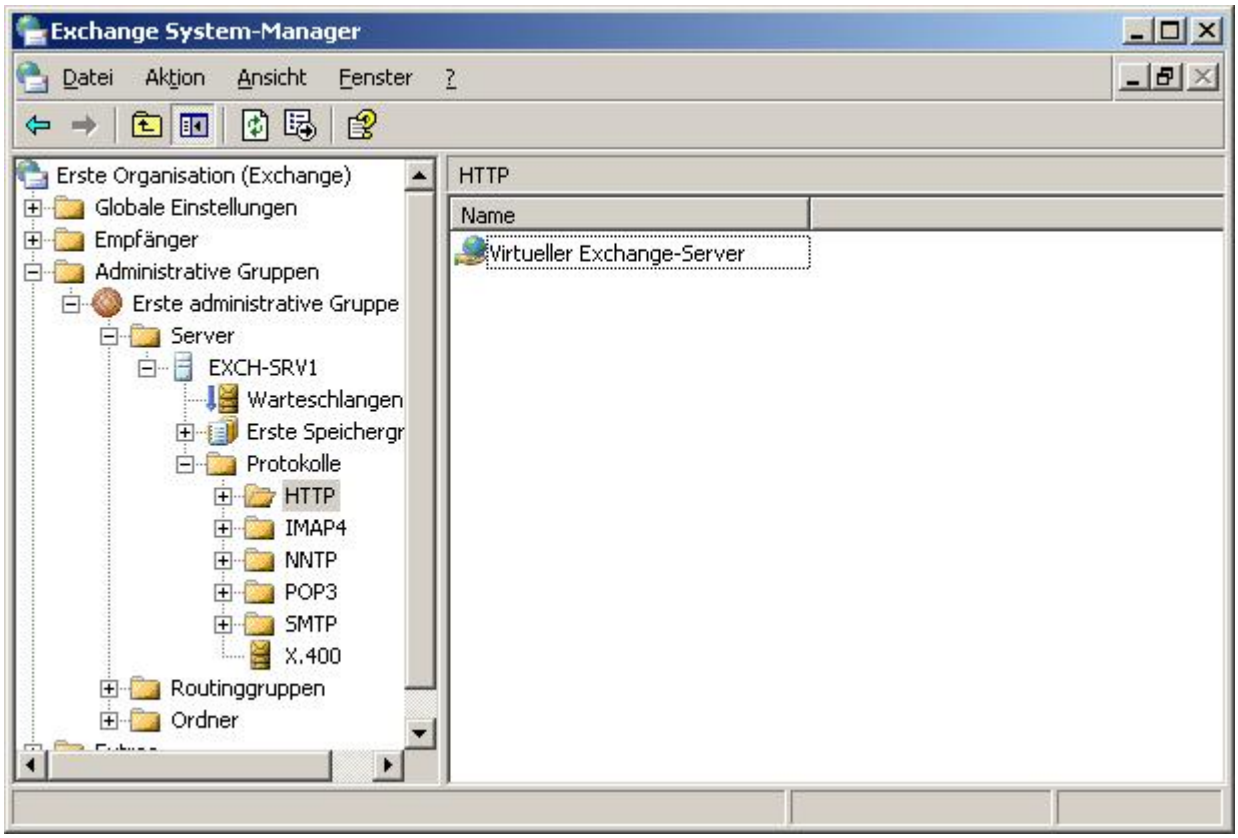
für die Verschlüsselung vom ISA- zum Exchange Server für exch-srv1.meinedomain.local, auf dem Exchange Server. Wichtig hierbei ist, dass der Client der Zertifizierungsstelle für das externe Zertifikat und der ISA Server der Zertifizierungsstelle des internen Zertifikates vertrauen. Des Weiteren müssen die FQDN's (Full Qualified Domain Name) mit denen der Zertifikate übereinstimmen und die Zertifikate dürfen nicht abgelaufen sein, ansonsten kommt kein Verbindungsaufbau zustande.

Voraussetzungen:

- Exchange Server ab Version 5.5 mit Standart Authentifizierung
- Ein Webserverzertifikat für exchange.meinedomain.de dem ISA Server
- Ein Webserverzertifikat für exch-srv1.meinedomain.local auf dem Exchange Server
- ISA Server 2004

1. Konfiguration des Exchange Servers

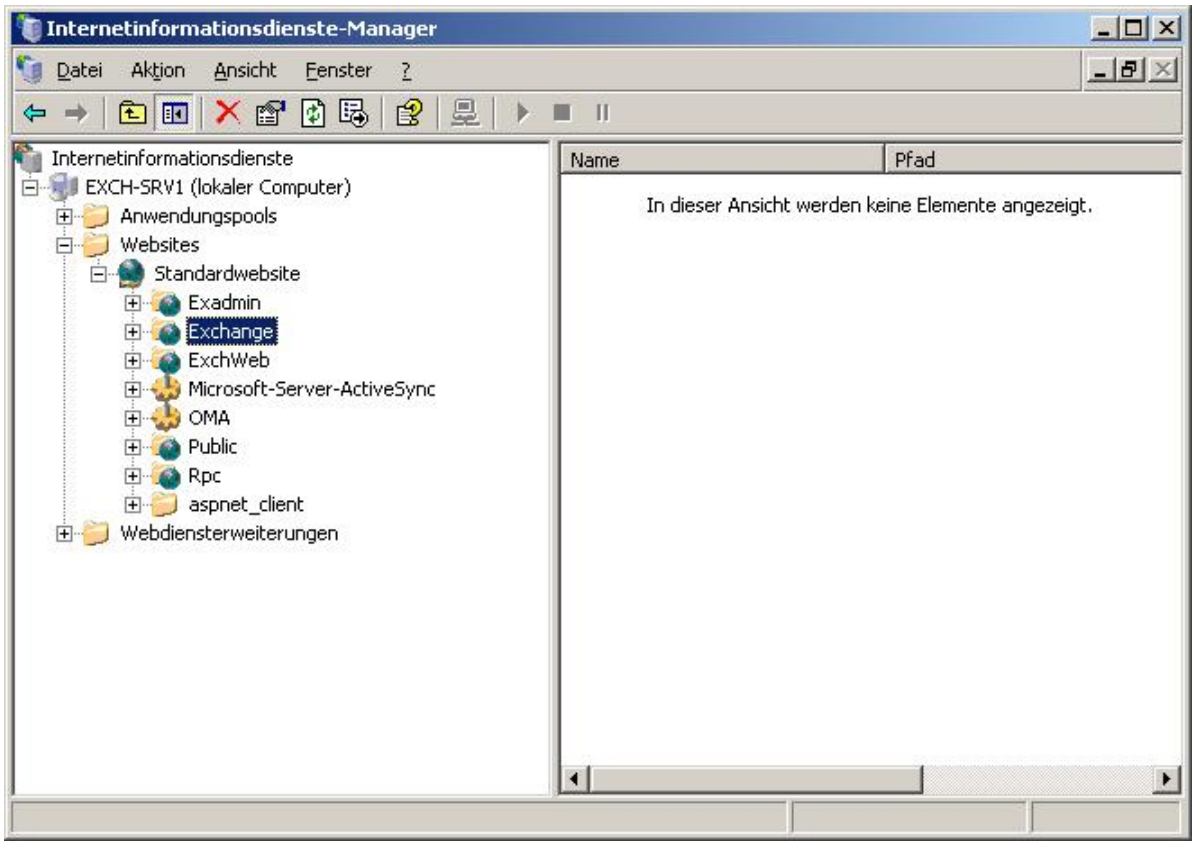
1.1 Konfiguration des HTTP Protokolls



Öffnen Sie, in der Verwaltungskonsole für den Exchange Server, die Einstellungen des virtuellen Exchange Servers für das HTTP Protokoll.

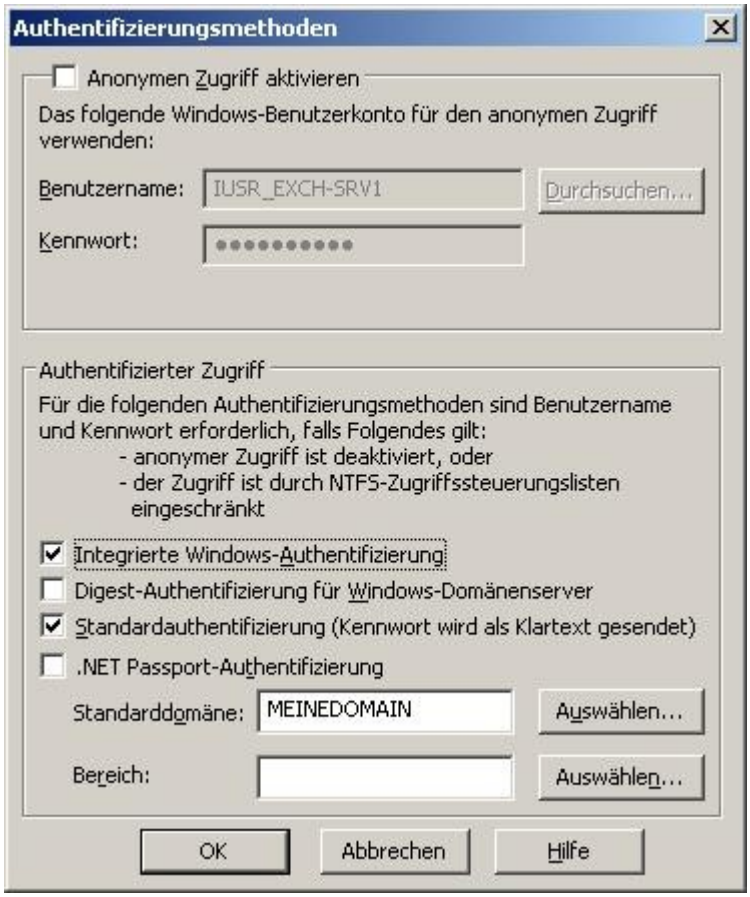
Unter dem Karteireiter Einstellungen deaktivieren Sie die Option *Formularbasierte Authentifizierung aktivieren*, da diese Authentifizierungsmethode nur an einer Stelle verwendet werden kann, in dieser Anleitung am ISA Server.

1.2 Konfiguration der virtuellen Verzeichnisse (Exchange, Exchweb, Public)

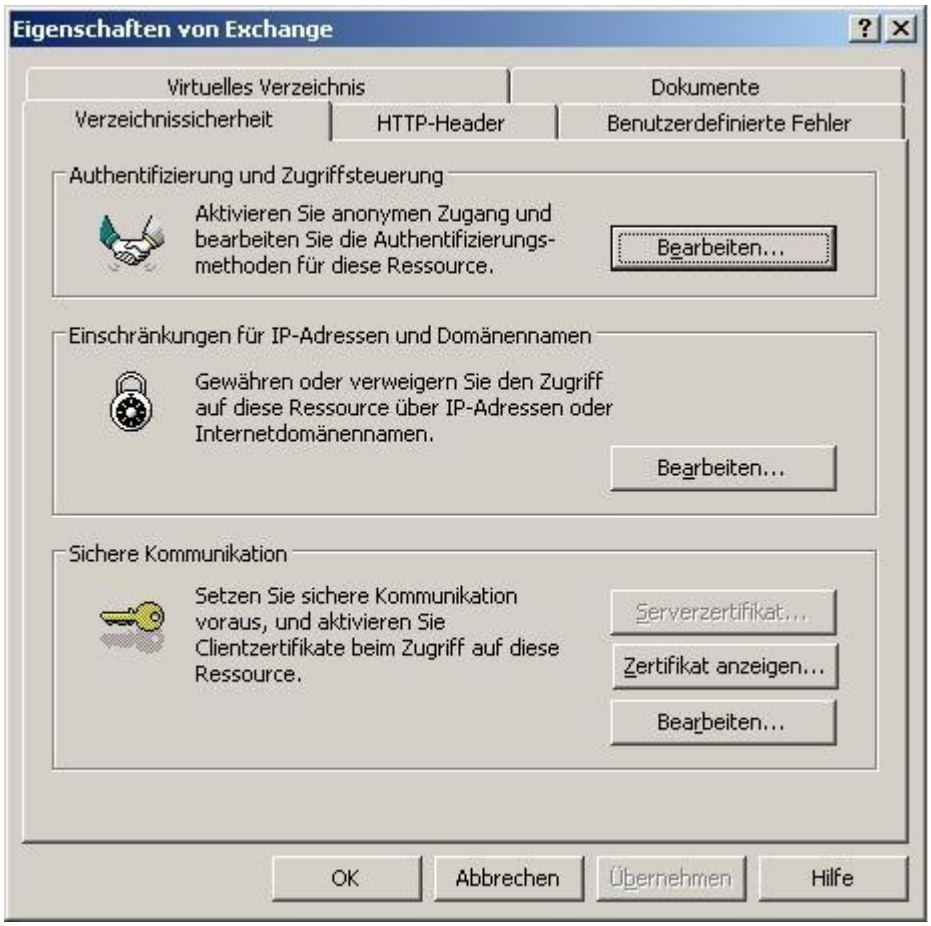


Konfigurieren Sie, wie folgend beschrieben, der Reihe nach die virtuellen Verzeichnisse Exchange, Exchweb und Public.

Unter dem Karteireiter Verzeichnissicherheit öffnen Sie über Bearbeiten zunächst die Authentifizierung und Zugriffssteuerung.



Setzen Sie die Authentifzierungsmehtode auf Standartauthentifzierung. Es erscheint eine Warnmeldung, die Sie bestätigen. Durch den verwendeten SSL Tunnel besteht für die Daten kein Sicherheitsrisiko. Die Authentifizierungsmethode Integriert können Sie für interne Zugriffe aktivert lassen, oder deaktivieren.



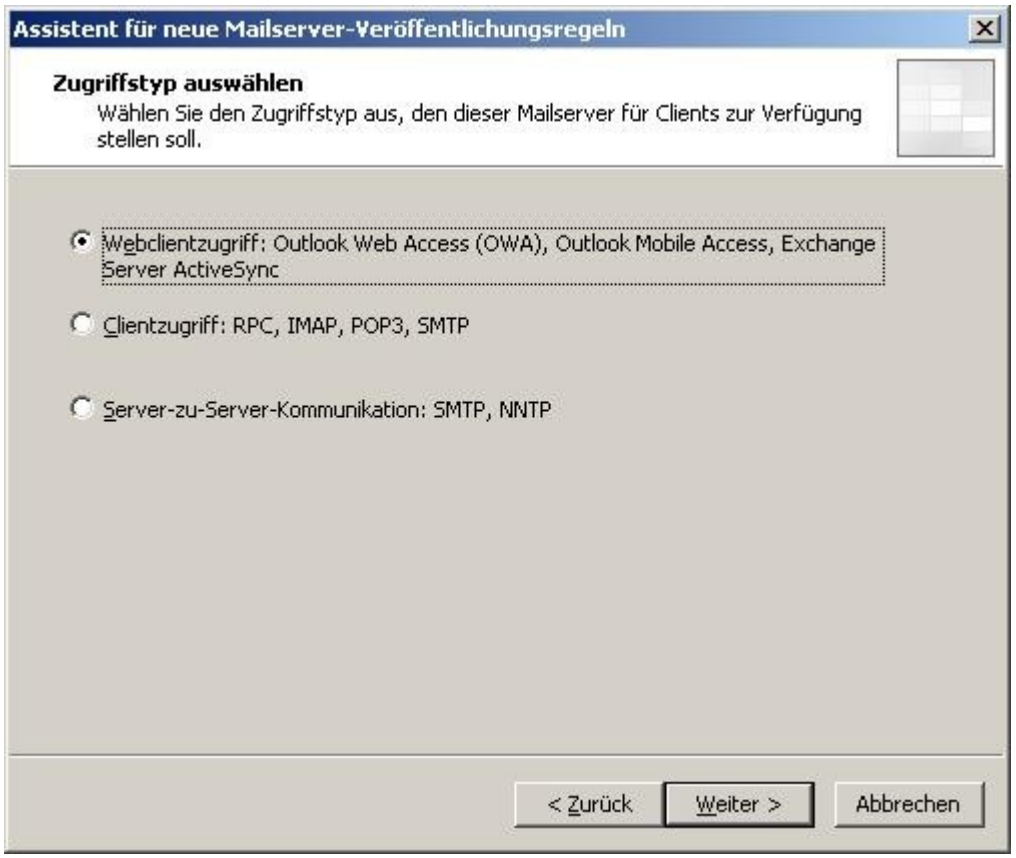
Abschließend können Sie unter der Option Sichere Kommunikation weitere Einstellungen bzgl. der SSL Verschlüsselung konfigurieren.

Setzen Sie den Haken bei Sichern Kanal voraussetzen (SSL), um Anfragen nur per SSL zu zulassen. Optional können Sie eine Verschlüsselungsstärke von 128 Bit fordern.

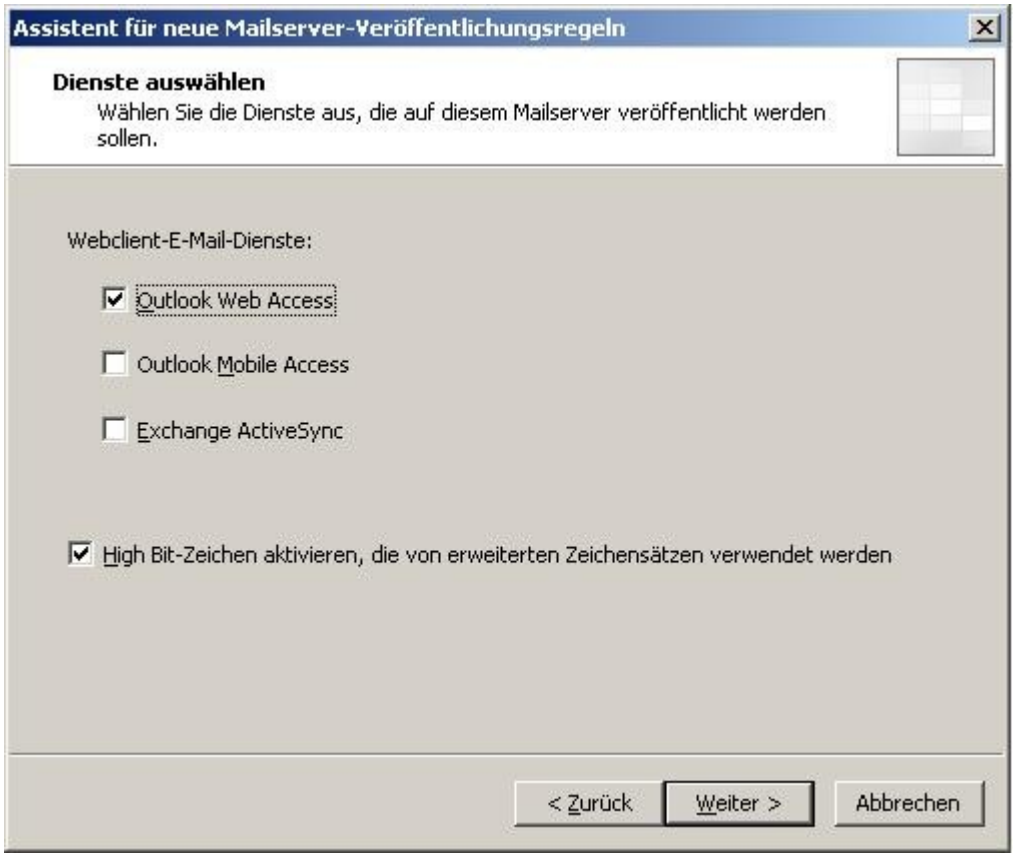
2. Konfiguration des ISA Servers 2004

2.1 Erstellen einer sicheren Webveröffentlichungsregel (Teil 1)

Erstellen Sie über Servername -> Firewallregeln -> Neu -> Mailserververöffentlichungsregel eine neue Veröffentlichungsregel. Es öffnet sich der Assistent zur erstellung einer neuen Firewallrichtlinie zur Veröffentlichung eines Mailservers. Vergeben Sie einen Namen für die Regel.



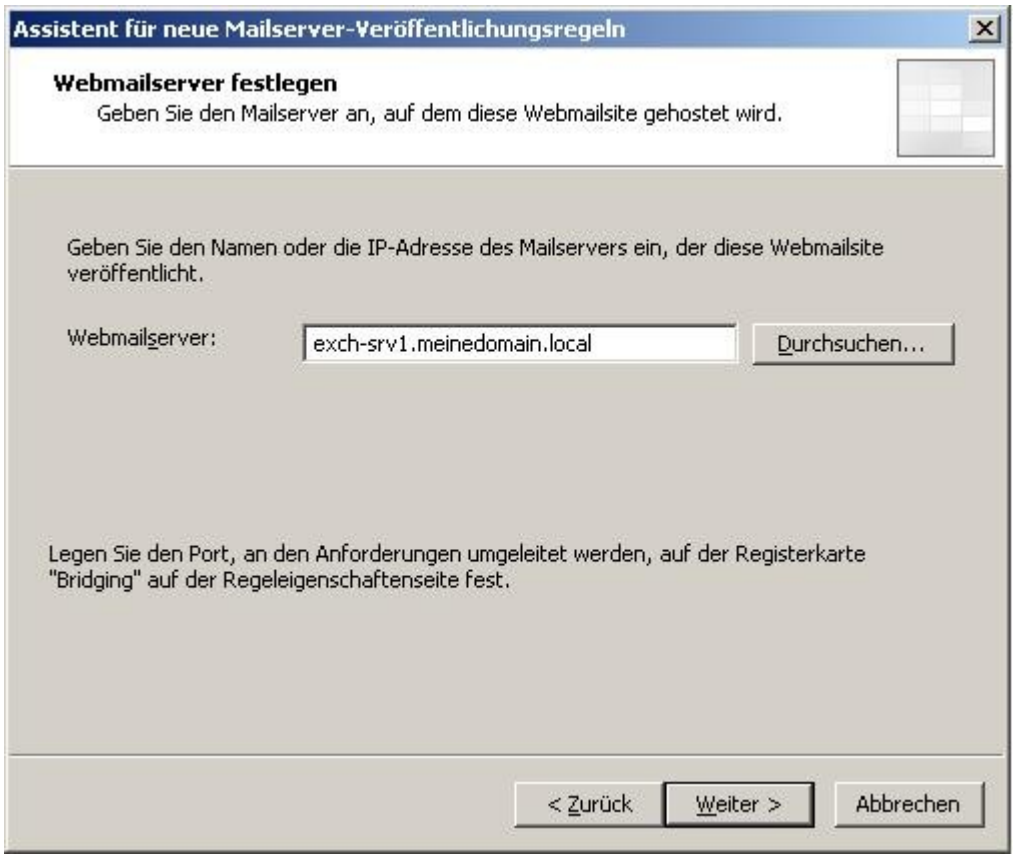
Wählen Sie die erste Option für den Webzugriff per OWA aus.



Als Webclient E-Mail Dienst wählen Sie Outlook Web Access aus. Die Option *High Bit*

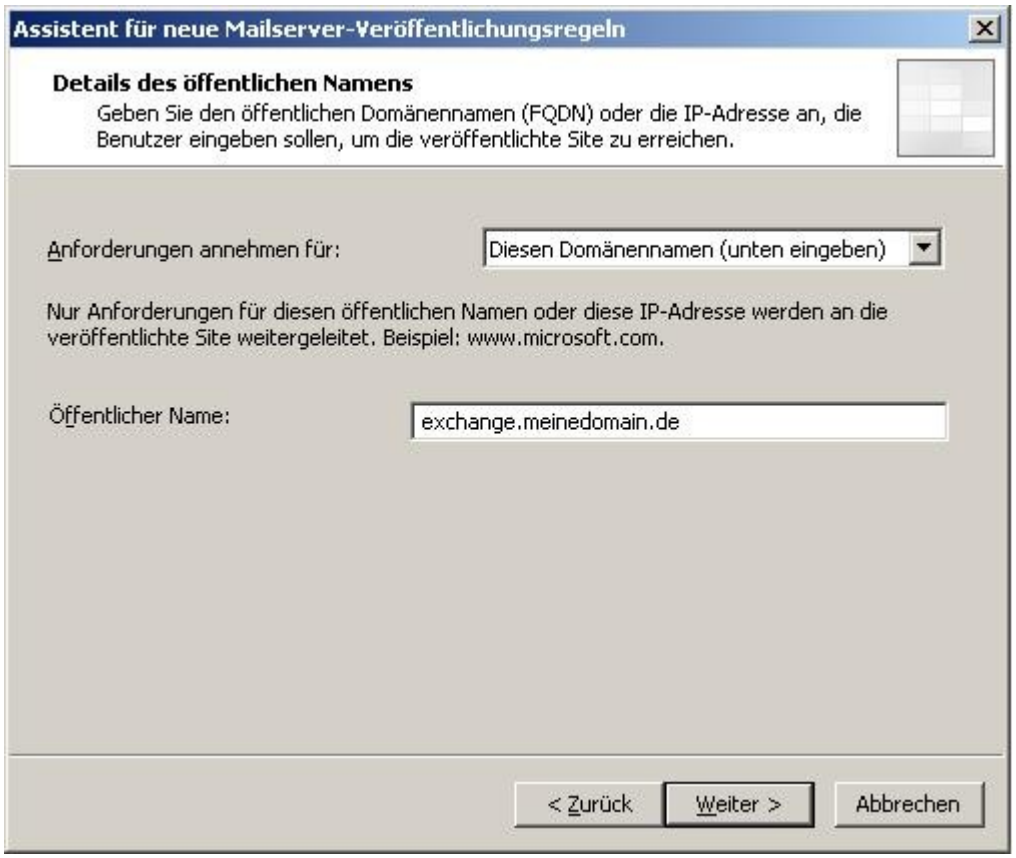
Zeichen aktivien muss aktiviert sein, da es ansonsten zu Problemen mit E-Mails bzw. Ordnern mit Umlauten kommt. Ist diese Auswahl nicht gesetzt, können Sie Z.B. keine neuen E-Mails schreiben, da diese erst im Ordner Entwürfe zwischen gespeichert werden.

Wählen Sie *Sichere Verbindung mit Client und Mailserver* aus, um einen SSL Tunnel zwischen Client und dem ISA Server und einen neuen SSL Tunnel zwischen ISA Server und dem Exchange Server herzustellen.



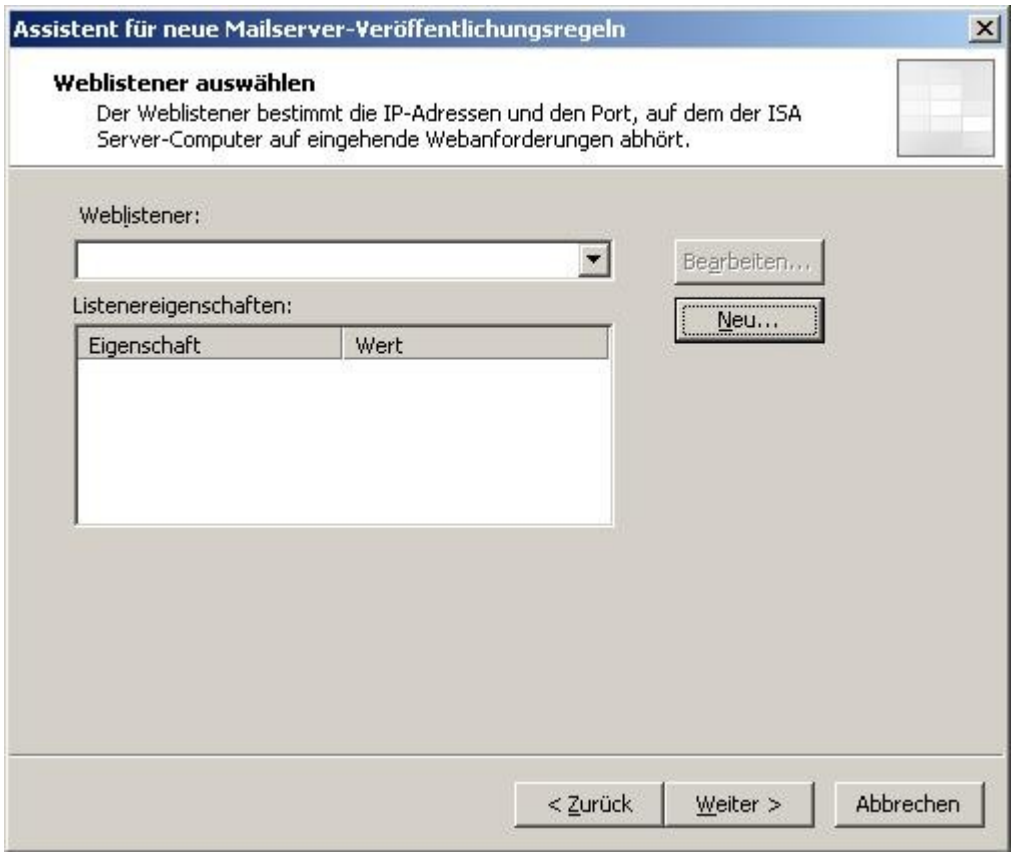
Geben Sie den Namen des internen Mailservers an.

Hinweis: Der Name des Zielservers muss mit dem FQDN des Zertifikates auf dem Exchange Server übereinstimmen. Sollte dies nicht der Fall sein, muss ein entsprechender Eintrag in der Hosts Datei auf dem ISA Server vorgenommen werden.



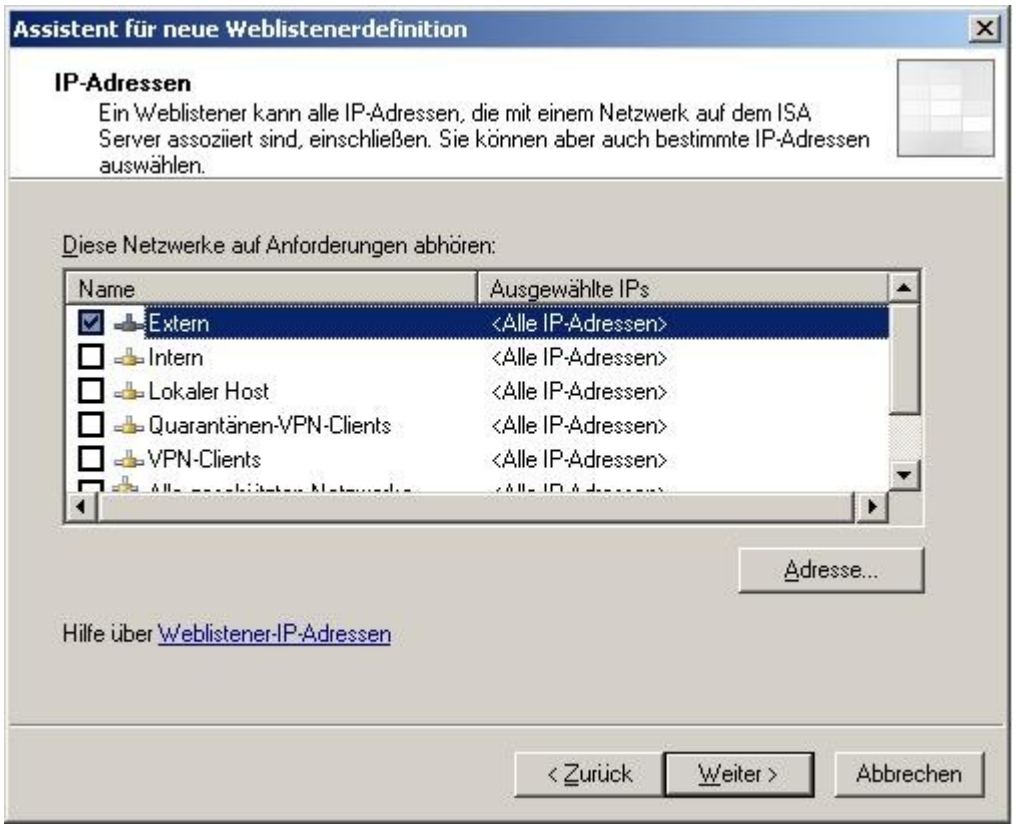
Geben Sie die URL an, unter der Ihr Outlook Webaccess von Extern zu erreichen ist.

2.2 Erstellen eines Weblisteners mit Formsbased Authentification

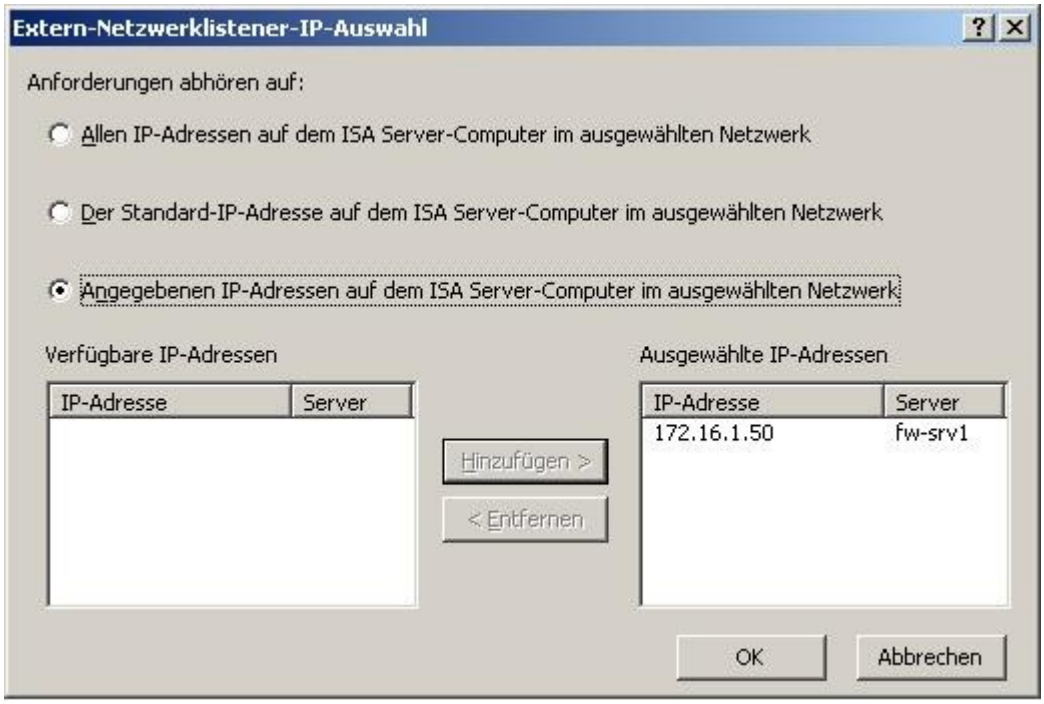


Erstellen Sie über den Button Neu einen neuen Weblistener.

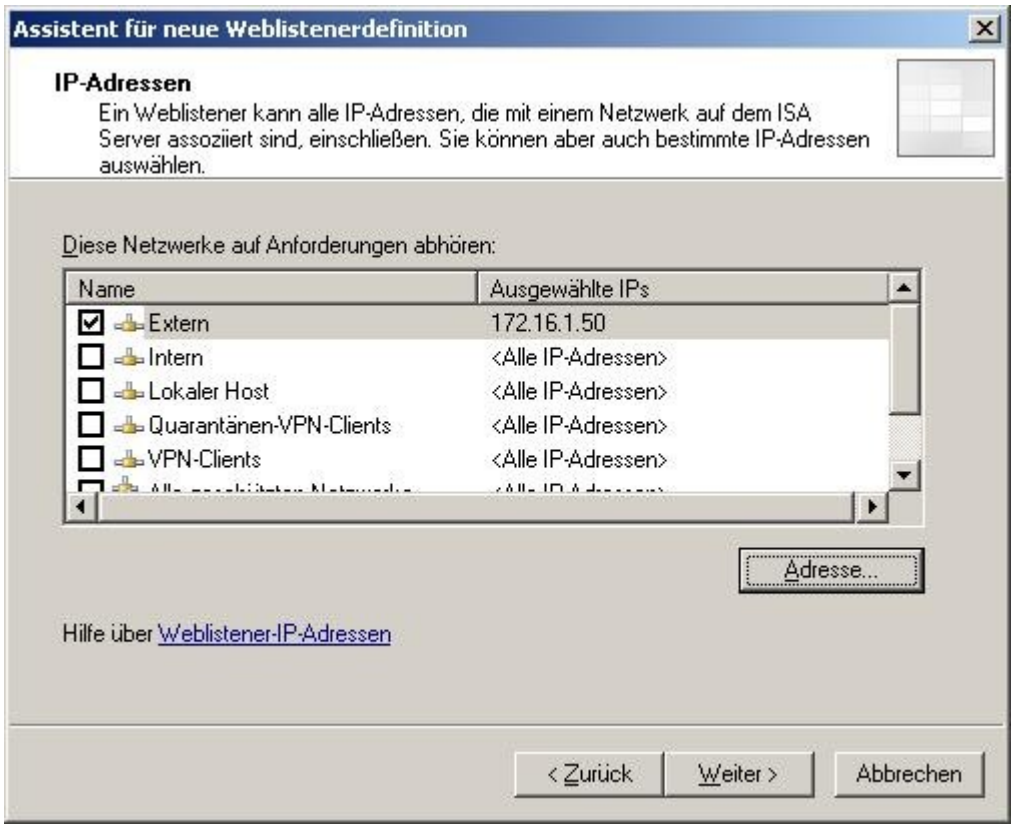
Vergeben Sie einen Namen für den Weblistener.



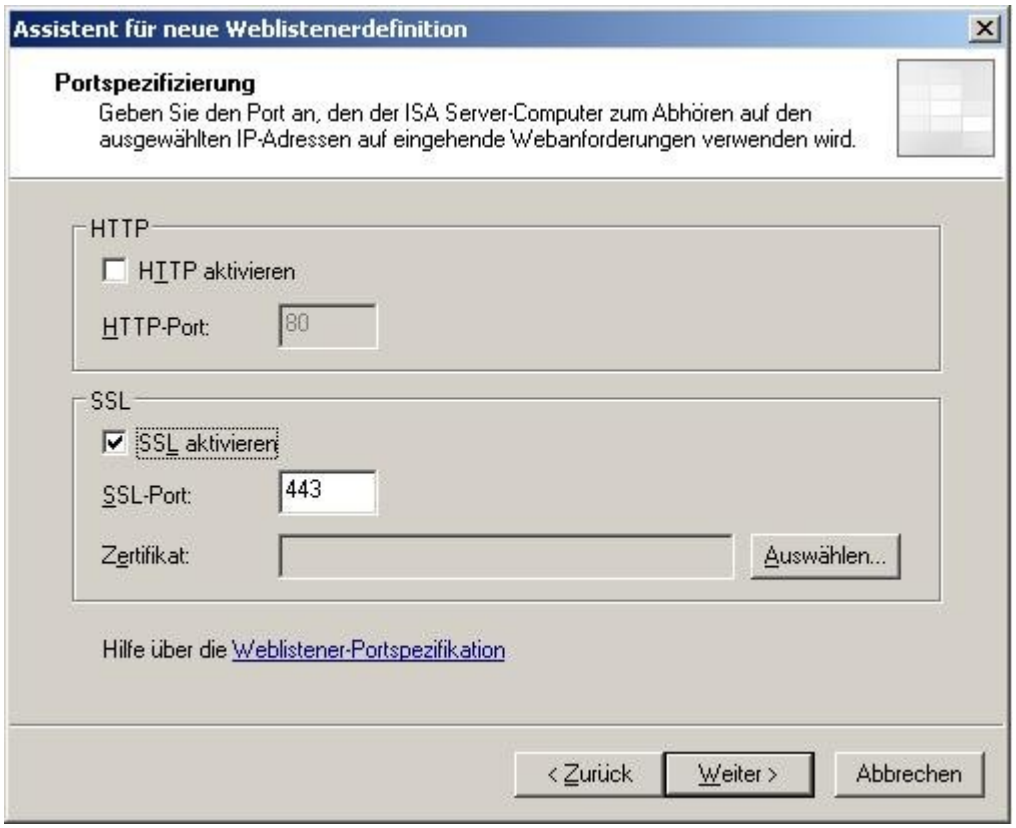
Geben Sie das Netzwerk an, von dem Zugriff zugelassen werden soll.



Wählen Sie die Option *Angegebenen IP-Adressen auf dem ISA Server-Computer im ausgewählten Netzwerk* aus, damit Sie die Möglichkeit haben eventuelle weitere Weblistener individuell zu konfigurieren. Fügen Sie die IP Adresse, auf der die Anfragen entgegengenommen werden sollen, hinzu.

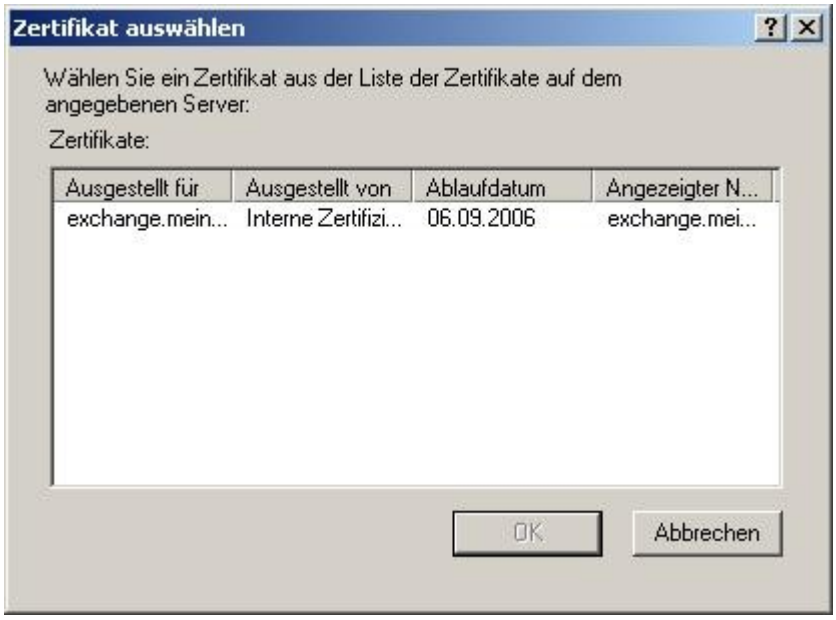


Unter dem ausgewählten Netzwerk sollte anschließend nur die angegebene IP Adresse ausgewählt sein.

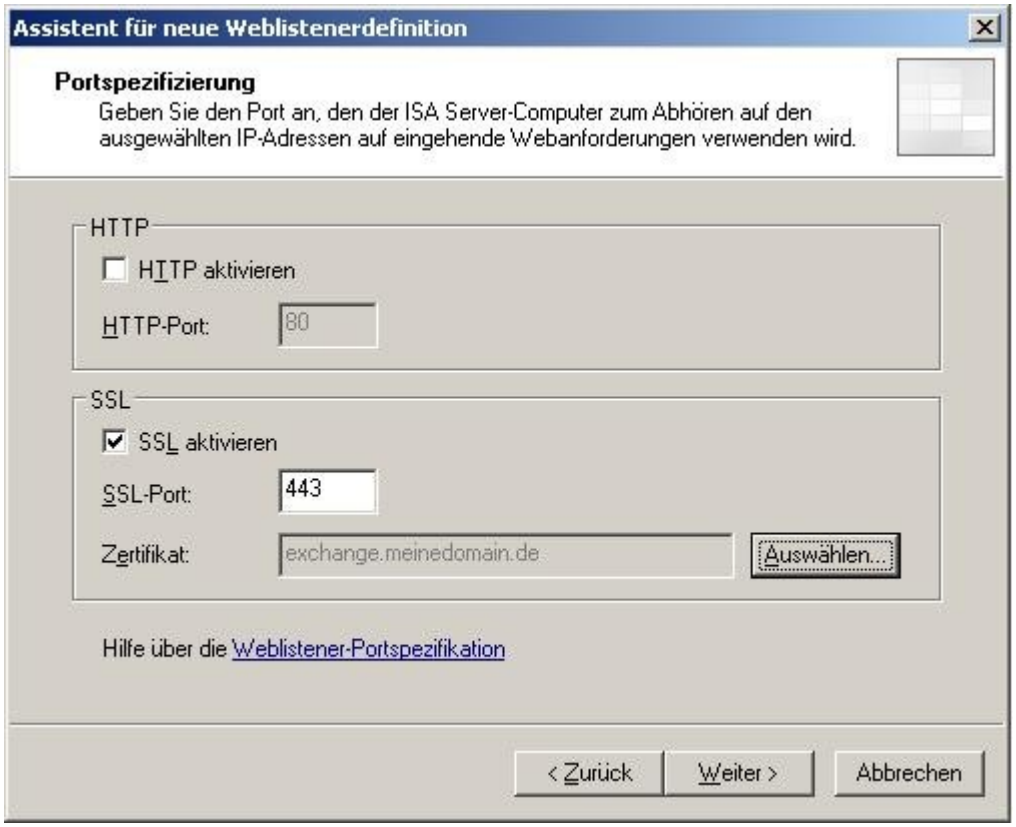


Deaktivieren Sie das Protokoll HTTP und aktivieren Sie das Protokoll SSL, um Anfragen nur über einen SSL Tunnel zu zulassen. Geben Sie über den Button Auswählen das Zertifikat für

die SSL Verschlüsselung an.



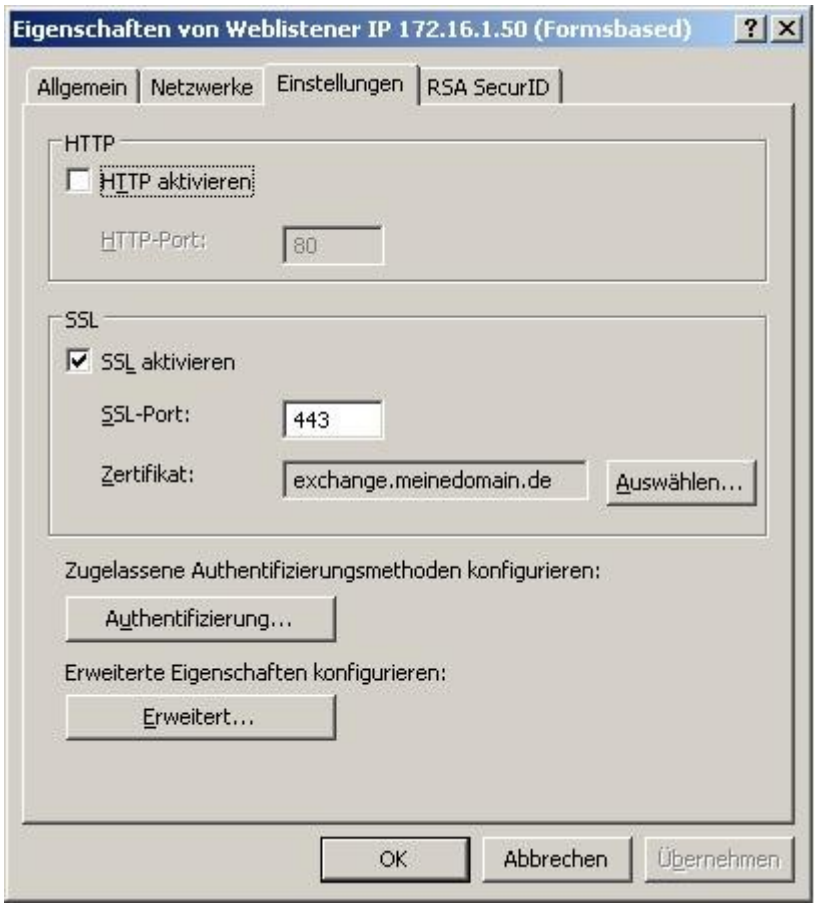
Wählen Sie das Zertifikat aus.



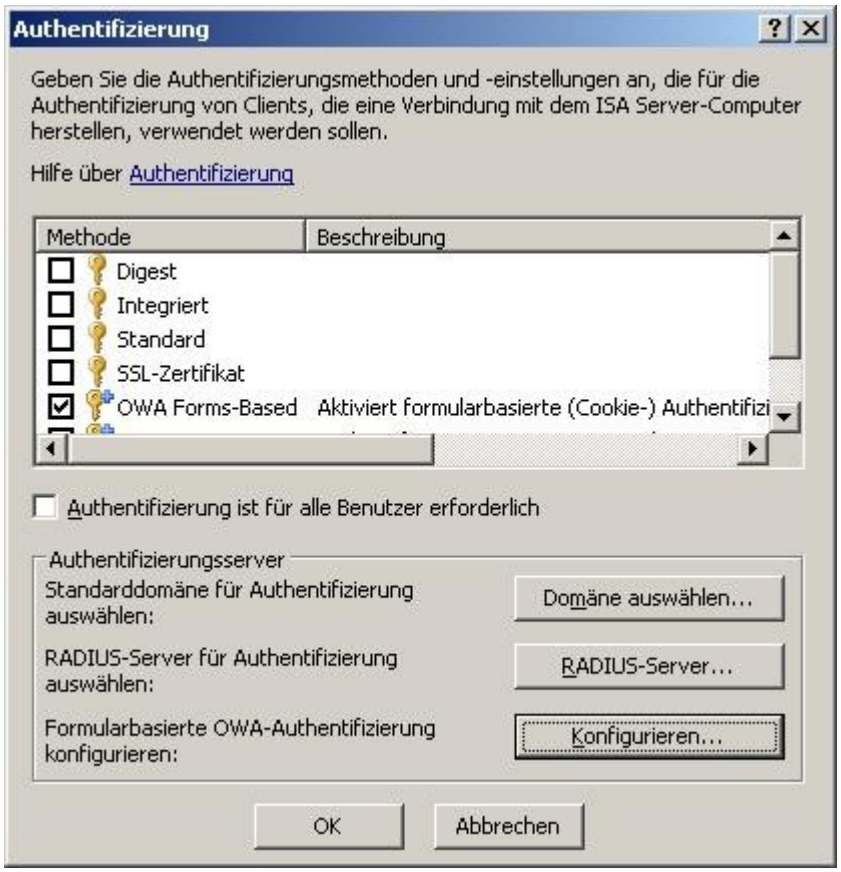
Anschließend sollte der Weblistener wie im Bild abgebildet konfiguriert sein.

Zum Abschluss bekommen Sie eine Zusammenfassung des Weblisteners angezeigt.

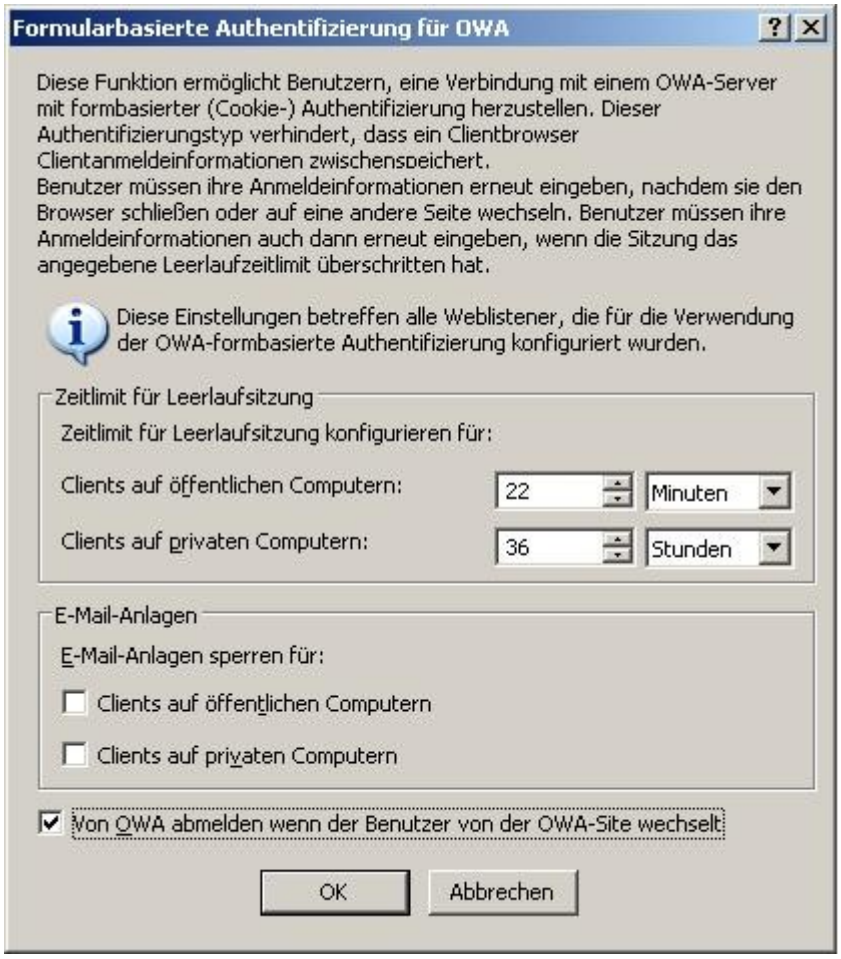
Ändern Sie die Authentizierungsmehtode von Integriert auf die Formularbasierte Authentifizierung über den Button Bearbeiten.



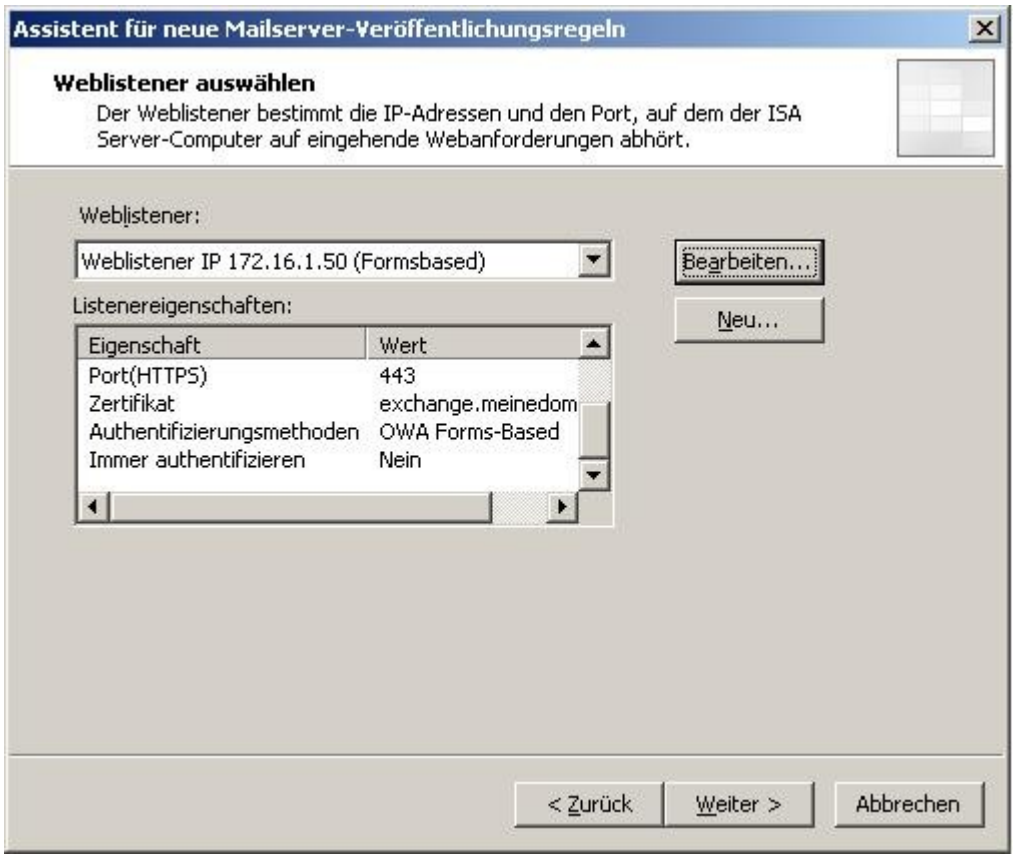
Öffnen Sie die Authentifzierungsmethoden über den Button Authentifizeriung.



Wählen Sie die Authentifzierungsmehtode *OWA Forms-Based* aus. Über Formularbasierte OWA Authentifizierung konfigurieren" können Sie weitere Einstellungen für die Authentizierungsmethode vornehmen.

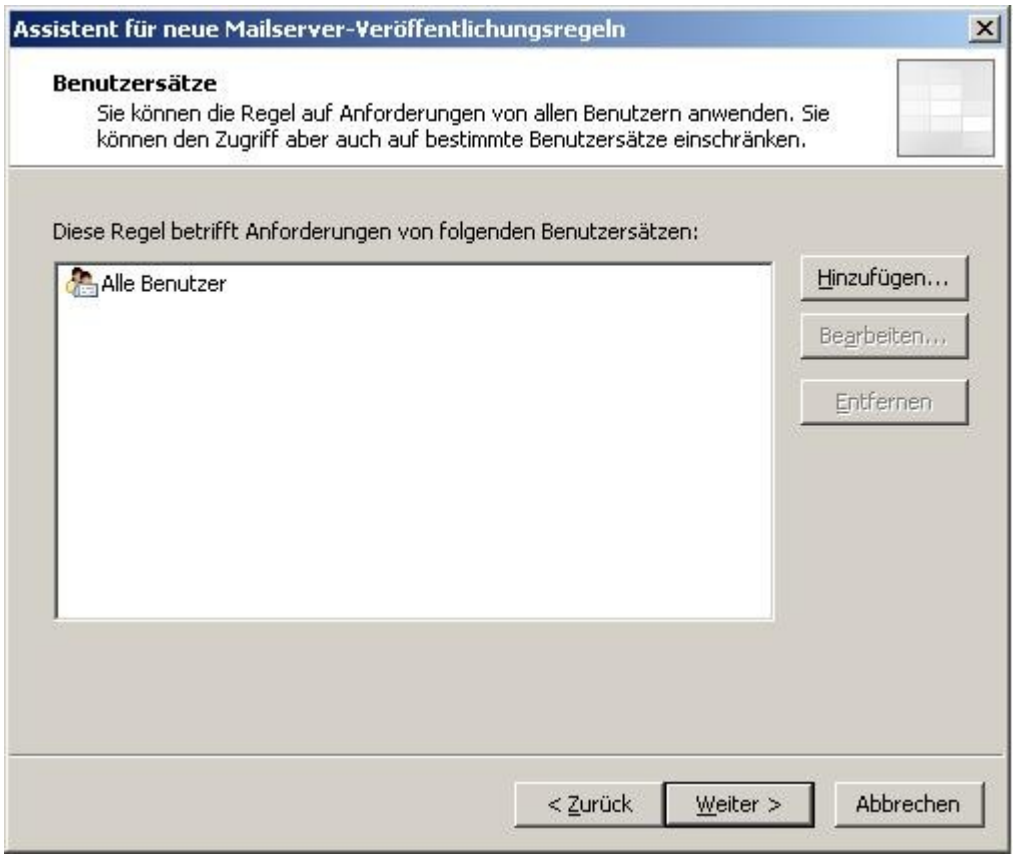


In diesem Fenster können Sie die Timeouts und die Behandlung von E-Mail Anlagen auf privaten bzw. öffentlichen Computern konfigurieren. Aktivieren Sie die Optoin *Von OWA Abmelden wenn der Benutzer von der OWA Site wechselt*, damit die Verbindung getrennt wird, sobald der Benutzer Outlook Webaccess verlässt. Diese Einstellungen sind die Grundlage für die Sicherheitsoptionen, die bei der Anmeldung ausgwählt werden können.



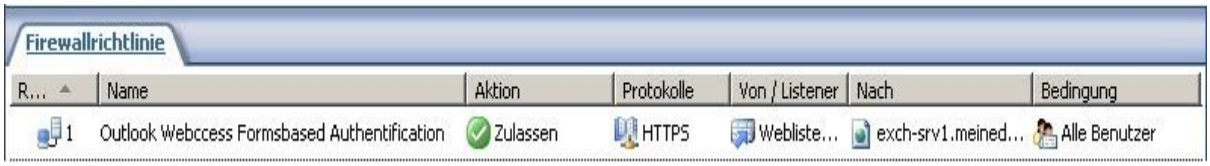
Die Konfiguration des Weblisteners ist nun abgeschlossen.

2.1 Erstellen einer sicheren Webveröffentlichungsregel (Teil 2)

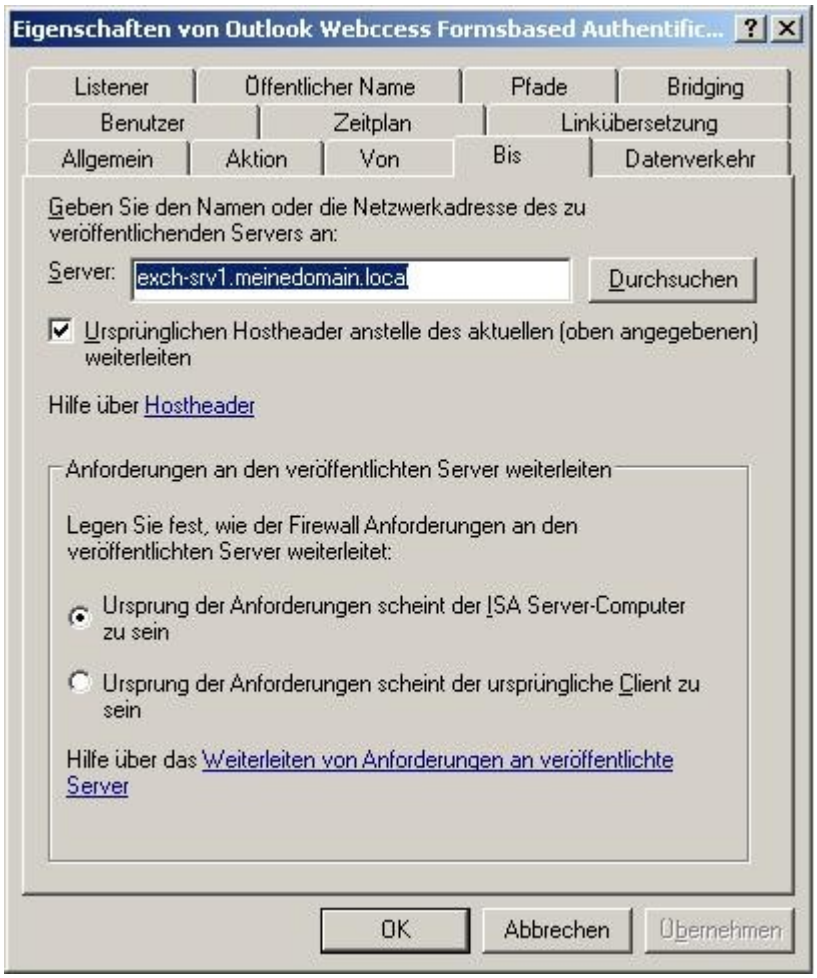


Hier könnten Sie den Zugriff auf eine bestimmte Benutzergruppe einschränken.

Zum Abschluss bekommen Sie eine Zusammenfassung der Veröffentlichungsregel angezeigt.

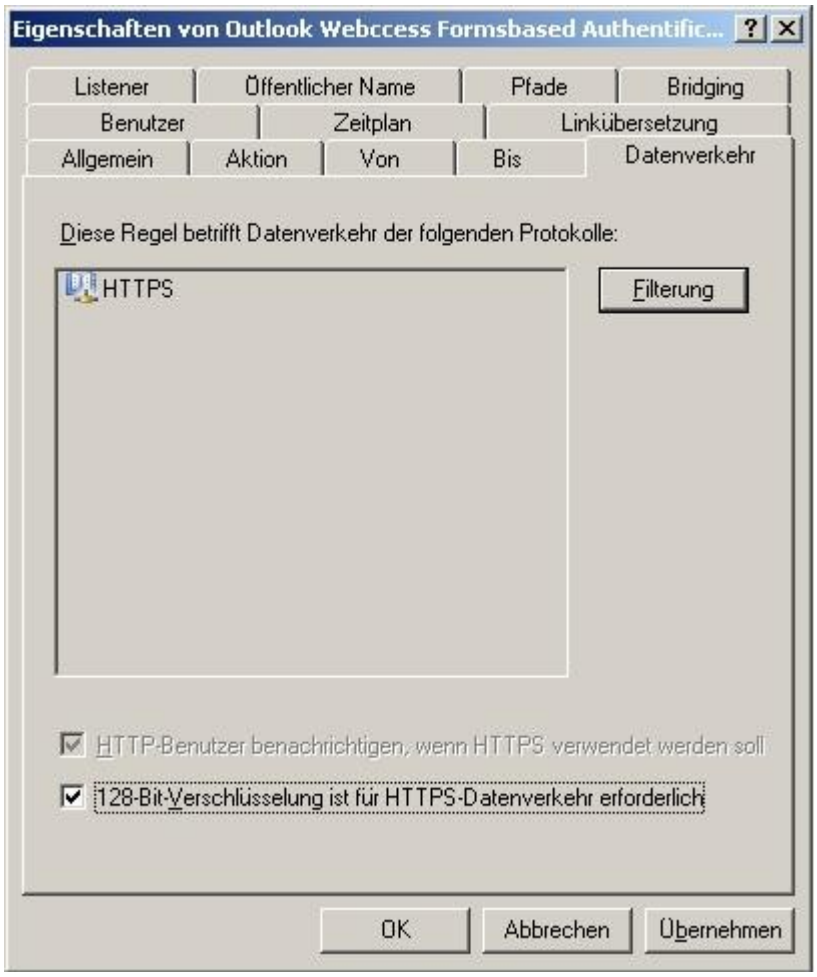


Öffnen Sie zur weiteren Konfiguration die Eigenschaften der Veröffentlichungsregel.



Unter dem Karteireiter Bis können Sie unter der Option *Anforderungen an den veröffentlichten Server weiterleiten* auswäheln, welche IP Afesse an den Exchange Server übermittelt werden soll. Dies kann für statistische Auswertungen oder zu Fehlersuche relevant sein.

- Ursprung der Anforderung scheint der ISA Server Computer zu sein, übermittelt, wie der ISA Server 2000, die interne IP Adresse des ISA Servers an den Exchange Server
- Ursprung der Anforderung scheint der ursprüngliche Client zu sein, reicht die IP Adresse des externen Clients an den Exchange Server durch.



Eine Verschlüsselungsstärke von 128 Bit kann unter dem Karteireiter Datenverkehr gefordert werden.

Geben Sie die externe URL mit dem Pfad /exchange/, in dieser Anleitung https://exchange.meinedomain.de/exchange, im Internet Explorer ein, um die Veröffentlichungsregel zu testen. Es erscheint die formularbasierte Anmeldemaske von Outlook Webaccess. Geben Sie Ihren Benutzernamen und das Kennwort ein, um sich anzumelden.

Zusätzlich haben Sie die Möglichkeit folgende Optionen zu sezten:

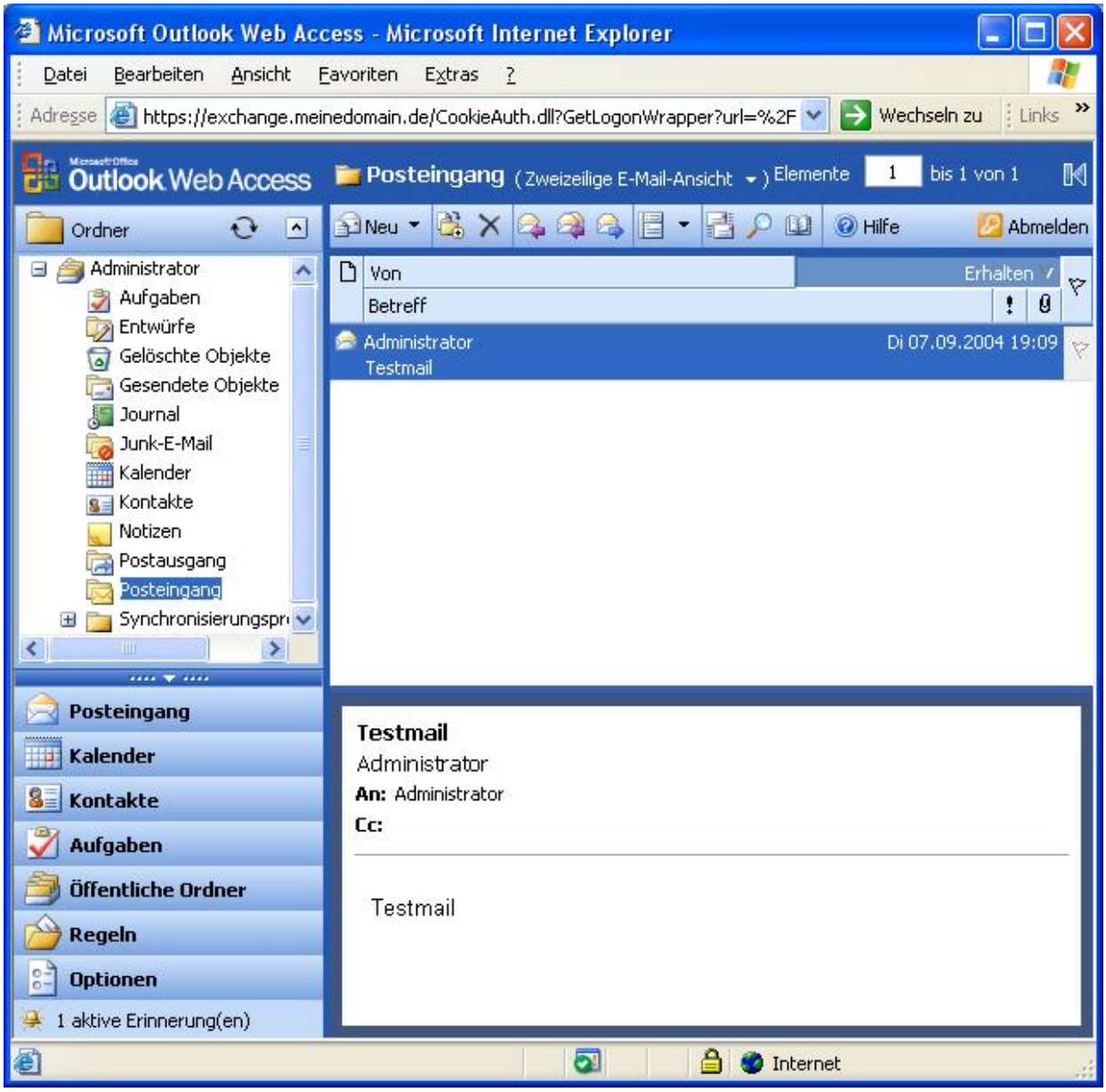
Client:

- Premium : Ihnen stehen alle Features von Outlook Webaccess zur Verfügung
- Standart : Stellt Ihnen eine abgespeckte Version von Outlook Webaccess zur Verfügung, mit weniger Features. Diese Methode ist für langsame Netzwerkverbindungen besser geeignet.

Sicherheit:

- Öffentlicher oder gemeinsam genutzter Computer : Verwendet die unter Kapitel 2.2 eingestellten Optionen (Timeout, E-Mail Anlagen) für einen öffentlichen Computer.

- Privater Computer: Verwendet die unter Kapitel 2.2 eingestellten Optionen (Timeout, E-Mail Anlagen) für einen privaten Computer



Nach erfolgreicher Anmeldung haben Sie Zugriff auf Ihr Postfach per Outlook Webaccess.

ISA Server 2004 – HTTP Filter

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

In diesem Artikel erläutere ich die Konfiguration des mit ISA 2004 mitgelieferten HTTP Filters und die interne Funktionalität. Für eine effiziente Arbeit mit dem HTTP Filter müssen Sie das HTTP Protokoll etwas verstehen. Lesen Sie dazu bitte folgenden Artikel.

Was ist ein Webfilter / HTTP-Filter

Webfilter sind DLLs, welche auf dem IIS ISAPI (Internet Server Application Programming Interface) Modell basieren. Webfilter werden vom Webproxy Filter geladen. Wenn ein Webfilter geladen ist, werden seine Informationen an den Webproxy Filter weitergeleitet. Dieser legt fest, welche Typen von Ereignissen überwacht werden sollen. Jedes Mal wenn ein solches Ereignis eintritt, wird der Webfilter benachrichtigt.

Die folgende Grafik zeigt den HTTP-Filter in den Add-Ins des ISA Server 2004.

Webfilter Funktionalität

Der Webfilter im ISA Server 2004 hat folgende Aufgaben:

- HTTP Anforderungen scannen und modifizieren
- HTTP Antworten scannen und modifizieren
- Blockieren von speziellen HTTP Antworten
- Netzwerkverkehr protokollieren und analysieren
- Datenverschlüsselung und Komprimierung
- Benutzerdefinierte Authentifizierungsschemata (OWA, RADIUS, RSA ID)

Wie funktioniert ein Webfilter

- Ein Client stellt eine Verbindung zum ISA Server 2004 her und fordert eine Ressource aus dem etxernen Netzwerk an.
- Die Firewall Engine führt Paketfiltering für die Anfrage durch und prüft, ob die Anforderung auf dieser Ebene erlaubt ist.
- Wenn die Anforderung erlaubt ist, wird eine Verbindung mit dem Firewall Dienst hergestellt.
- Der Firewall Dienst überprüft die Firewallregel, ob ein Applikations- oder Webfilter für die Regel definiert ist.
- Wenn das der Fall ist (HTTP/HTTPS), übergibt der Firewall Dienst die Anforderung an den Webproxy Filter.
- Die Anfrage wird basierend auf der Webfilter Konfiguration überprüft. Der Webfilter erlaubt oder verweigert die Anforderung.
- Wenn die Anfrage vom Webfilter akzeptiert wurde, wir die Anfrage zurück an den Firewall Dienst übergeben und über das Netzwerkinterface an den Zielserver weitergeleitet.

Wichtig:

Der HTTP Filter im ISA Server 2004 ist regelspezifisch, dass heißt, Sie können den HTTP Filter pro Firewallregel konfigurieren.
Einzige Ausnahme von der Regel: Die Angabe der **maximalen Header-Länge** im Feld **Anwendungsheader** ist für alle HTTP Policies gültig. Eine Änderung die Sie hier vornehmen, gilt für alle Policies.

Bemerkung:

Der HTTP Filter im ISA Server 2004 kann auch HTTPS Datenverkehr filtern, wenn es sich bei dem Datenverkehr um eine sichere Webserververöffentlichung handelt, bei der die Anfrage im so genannten Bridge Mode betrieben wird. Im Bridge Mode wird die HTTPS Anfrage am ISA Server aufgehoben und vom ISA Server erneut SSL verschlüsselt und an den Client (z. B. internen Webserver gesendet). Im SSL Tunnelmodus (explizite SSL Verbindung zwischen Client und externem Server) ist keine Webfilterung möglich. Sie müssen dazu Software von Drittanbietern verwenden.

HTTP Filter Konfiguration

Klicken Sie jetzt auf "HTTP konfigurieren" in der entsprechenden Firewallregel.

Anforderungsheader:

Maximale Headerlänge (Bytes): Gibt die maximale Anzahl an Bytes im Header (URL und Header) für einen **HTTP Request** an, bevor der Request geblockt wird. Starten Sie mit einem Limit von 10.000 Bytes und erhöhen Sie den Wert nur, wenn Sie Probleme bei dem Aufrufen von Webseiten feststellen.

Anforderungsnutzlast:

Maximale Nutzlastlänge (Bytes): Per Default wird jede Nutzlastlänge zugelassen, sie können die Länge aber auch auf Anzahl XX Bytes beschränken. Mit Hilfe dieses Parameters können Sie die Anzahl der Daten beschränken, welche ein Benutzer per **HTTP POST** an Ihre Webseite in einem Webserververöffentlichungsszenario überträgt.

URL-Schutz:

Maximale URL-Länge (Bytes): Spezifiziert die maximale Länge einer erlaubten URL. Der Default Wert ist 10.240 Byte. Reduzieren Sie die Länge nur, wenn ein Angriff mit überlangen URLs bekannt wird.
Maximale Abfragelänge (Bytes): Spezifiziert die maximale Länge einer URL Abfrage. Eine URL Abfrage erkennen Sie an den Zeichen nach dem **?** in einer URL
Normalisierung verifizieren: Webserver empfangen Anfragen, welche als URL kodiert sind, dass heisst, diese Anfragen können auch Zeichen enthalten, welche mit einem **%** Zeichen, gefolgt durch eine Nummer, ersetzt werden müssen. Als Normalisierung bezeichnet man den Prozess der Decodierung von URL kodierten Anfragen. Weil das **%** Zeichen selbst URL kodiert sein kann, kann ein Angreifer einen **URL Request** an einen Webserver schicken,

welcher doppelt kodiert ist. Wenn Sie **"Normalisierung verifizieren"** ausgewählt haben, normalisiert der HTTP Filter die URL doppelt und wenn er beim zweiten mal einen Unterschied in der URL feststellt, wird der Request verworfen.
High Bit Zeichen sperren: URLs welche Double Byte Character (DBCS) oder Latin1 enthalten, werden geblockt wenn diese Einstellung aktiv ist. Das sperrt in der Regel Sprachen, welche mehr als 8 Bit (also 16 Bit) zur Darstellung aller Zeichen Ihrer Sprache benötigen. Seien Sie mit der Aktivierung dieses Features vorsichtig, gerade in OWA Szenarien führt das unter Umständen zu Problemen.

Ausführbare Dateien

Antworten sperren, die von Windows ausführbaren Inhalt enthalten: Diese Option blockiert sämtlichen von Windows ausführbaren Inhalt (Antworten welche mit einem MZ (z. B. EXE) beginnen). Der HTTP Filter erkennt hier übrigens auch umbenannte EXE Dateien in z. B. .DOC Dateien anhand des Dateityps.

Als nächstes können Sie die zugelassenen HTTP-Methoden konfigurieren.

Beispiele für HTTP Methoden:

GET - Empfängt die spezifizierte URI
HEAD - Empfängt nur den Header im URI
POST - Fragt den Server an, die Informationen zu akzeptieren
PUT - Fragt den Server an, die Informationen und den spezifizierten URI zu akzeptierenj
DELETE - Fragt den Server an, die spezifizierte URI zu löschen

In diesem Beispiel blocken wir HTTP Anfragen mit der **HTTP PUT** Methode

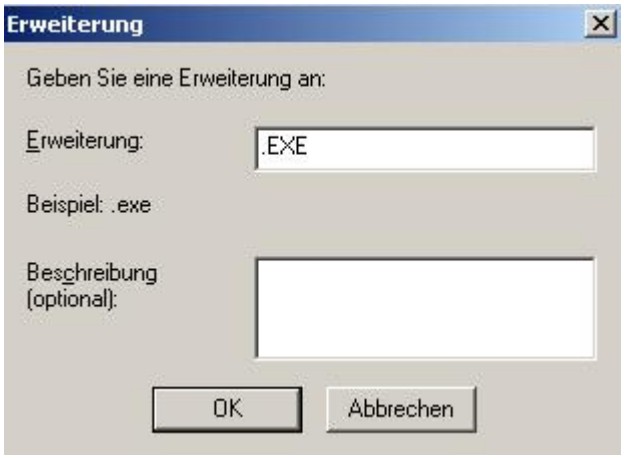
Mit Hilfe des geblockten **HTTP PUT** können interne Clients keine Daten mehr zu externen Webseiten posten. Das kann sinnvoll sein um zu verhindern, das sensitive Informationen nicht auf anderen Webseiten veröffentlicht werden können, aber auch in Webveröffentlichungsszenarien kann dieses Feature sinnvoll sein um zu verhindern, dass Angreifer Malicious Informationen auf der internen Webseite posten können.

Dateiendungen sperren

Mit Hilfe der Möglichkeit zur Sperrung von bestimmten Dateiendungen im HTTP Filter, können Sie einfach und effektiv z. B. das Downloaden von **.EXE** Dateien verhindern.

Anforderungen sperren, die mehrdeutige Erweiterungen enthalten, blockiert alle Extensionen, bei welchen der ISA Server die Erweiterung nicht bestimmen kann.

In diesem Beispiel blocken wir den Zugriff auf **.EXE** Dateien.



Wie arbeitet der ISA Server 2004 HTTP Filter Dateiendungen ab:

Wenn die Filterung basierend auf Dateiendungen aktiviert ist, überprüft der HTTP Filter jede Anfrage basierend auf der Dateiextension.
ISA Server interpretiert eine Dateiendung in einer URL nach dem letzten darin enthaltenen **Punkt** und einem **/** oder **?** oder dem Ende einer URL wenn kein **/** oder **?** enthalten ist.
Zusätzlich versucht der HTTP Filter Zeichen, welche einem **Punkt** folgen, als Dateierweiterung zu erkennen (z. B. EXE, DLL oder COM).
Wenn mehrere dieser Zeichen in einer URL enthalten sind, evaluiert ISA nur die erste Extension.

Um das zu verdeutlichen, einige Beispiele:

http://server/pfad/datei.ext	.ext wird geblockt
http://server/pfad/datei.htm/subpfad//msisafaq.asp	.asp wird geblockt
http://server/pfad.exe/datei.ext	.exe wird geblockt

Um im dritten Beispiel auch die **.EXT** Erweiterung zu verweigern, erstellen Sie eine Signatur, welche die **.EXT** Erweiterung in der URL verweigert.

HTTP Header Behandlung

Wenn ein Client eine Anforderung an den Webserver sendet oder der Webserver antwortet, ist der erste Part einer solchen Antwort immer ein **HTTP Request** oder **HTTP Response.**
Nach dem **HTTP Request** oder **Response**, sendet der Client oder der Server einen **HTTP Header**. Das **Request Header Feld** erlaubt dem Client zusätzliche Informationen über den **Request** an den Server mitzugeben.
Headers enthalten Informationen über den Client (Browser und Betriebssysteminformationen, Authorisierungsinformationen uvm.). Der **Client Header** verwendet auch das Attribut **User-Agent** mit welchem bestimmt werden kann, welche Applikation die Anforderung durchführt.

Mit Hilfe des HTTP Filters können jetzt z. B. bestimmte Header geblockt werden.

Sie können im Feld Serverheader auch noch festlegen, ob der Header aus der Antwort gelöscht werden soll oder der Header in der Antwort bearbeitet werden soll.

In diesem Beispiel blocken wir den **HTTP Header** für **Kazaa**. Somit werden Anforderungen, welche im Anforderungsheader diesen HTTP-Header enthalten, blockiert.

HTTP Filter Signaturen

Eine HTTP Signatur kann jedes Zeichen in einem **HTTP Body** oder **HTTP Header** sein. Sie können HTTP Signaturen dazu verwenden, z. B. das Ausführen von Applikationen zu verhindern. Um eine HTTP Signatur zu ermitteln, müssen Sie wissen, welche Muster die Applikation im **Request Header**, **Response Header** und **Body** verwendet und dann eine Signatur erstellen, welche Pakete basierend auf diesem String blockiert.

Die Schwierigkeit ist es, eine Signatur zu erstellen, die wirklich nur "schadhafte" Aufrufe blockiert. Wenn Sie z. B. eine Signatur erstellen, welche das Wort Mozilla blockiert, werden die meisten Webbrowser und Applikationen blockiert, weil die meisten Browser Mozilla kompatibel sind.

Um den MSN Messenger zu blockieren, konfigurieren Sie den **User-Agent:MSN Messenger** in einem **Request Header**.

Sie können aber auch den Zugriff auf Webseiten mit bestimmten Malicious Code verbieten indem Sie z. B. die Zeichenfolge **<iframe src="?"/>** blockieren. Diese Zeichenfolge veranlasst den Internet Explorer CPU Ressourcen zu verwenden.

Wichtig:

HTTP Signature Filtering funktioniert nur, wenn die **Requests** und **Responses** UTF-8 (eine Transformation von Unicode) codiert sind. Wird ein anderes Kodierungsschema verwendet, kann kein Signature Blocking durchgeführt werden.

In diesem Beispiel blocken wir den MSN Messenger mit Hilfe einer HTTP Signatur.

Zum Glück müssen Sie nicht jeden HTTP Filter selbst erstellen. Sie können im Internet diverse Filter Signaturen downloaden. Achten Sie bei dem Download jedoch darauf, dass diese Informationen aus vertrauenswürdigen Quellen stammen.

Sie finden hier eine Übersicht über ISA Server 2004 HTTP Filter Signaturen.
Eine Übersicht über typische Applikations-Signaturen finden Sie hier.

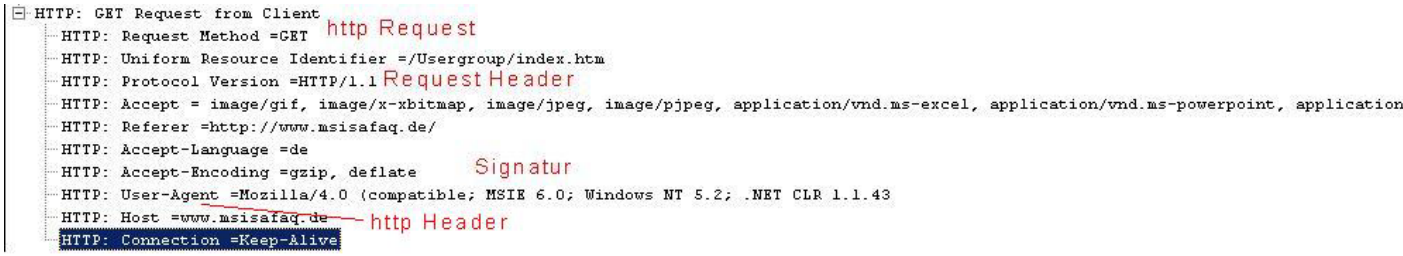
Wichtig:

Per Default scannt der Webfilter nur die ersten 100 Bytes im **Request** oder **Response** Body. Sie können den Wert erhöhen. Beachten Sie dabei allerdings, dass die Performance des Servers darunter leiden kann.

Ergebnis einer geblockten Verbindung durch den HTTP-Filter

Ermittlung von HTTP Anwendungsignaturen

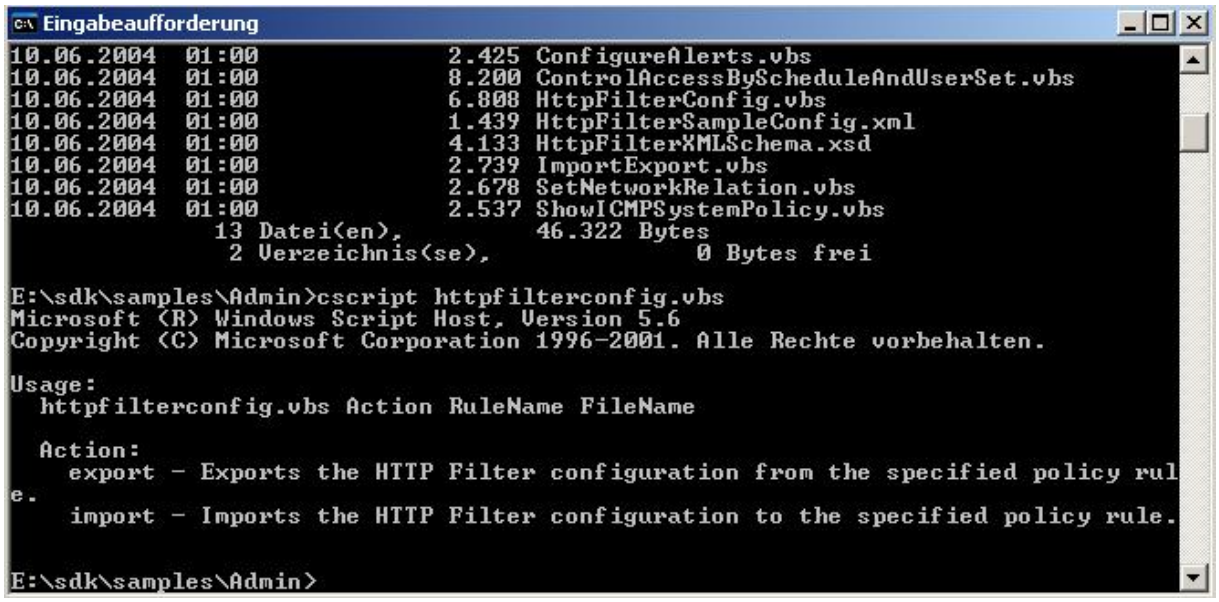
Zur Ermittlung von HTTP Anwendungssignaturen, die Ihnen nicht bekannt sind, können Sie den Windows eigenen Netzwerkmonitor verwenden und den Netzwerkverkehr sniffen.
Die folgende Grafik zeigt ein Beispiel für einen Netzwerksniff mit dem in Windows 2000/2003 verfügbaren Netzwerkmonitor. Sie können natürlich auch jeden anderen Netzwerkmonitor, zum Beispiel Ethereal verwenden.



Dieses Beispiel zeigt den HTTP Request Typen (GET), den HTTP Request Header (HTTP/1.1) den User-Agent (Mozilla/4.0) und die Signatur (MSIE 6.0).

HTTPFILTERCONFIG.VBS

Verwenden Sie HTTPFILTERCONFIG.VBS aus dem Verzeichnis \SDK\SAMPLES\ADMIN von der ISA Server 2004 CD um HTTP Filter zu importieren und zu exportieren.


Eingabeaufforderung
10.06.2004 01:00 2.425 ConfigureAlerts.vbs
10.06.2004 01:00 8.200 ControlAccessByScheduleAndUserSet.vbs
10.06.2004 01:00 6.808 HttpFilterConfig.vbs
10.06.2004 01:00 1.439 HttpFilterSampleConfig.xml
10.06.2004 01:00 4.133 HttpFilterXMLSchema.xsd
10.06.2004 01:00 2.739 ImportExport.vbs
10.06.2004 01:00 2.678 SetNetworkRelation.vbs
10.06.2004 01:00 2.537 ShowICMPSystemPolicy.vbs
13 Datei(en), 46.322 Bytes
2 Verzeichnis(se), 0 Bytes frei
E:\sdk\samples\Admin>cscript httpfilterconfig.vbs
Microsoft (R) Windows Script Host, Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. Alle Rechte vorbehalten.
Usage:
httpfilterconfig.vbs Action RuleName FileName
Action:
export - Exports the HTTP Filter configuration from the specified policy rul
e.
import - Imports the HTTP Filter configuration to the specified policy rule.
E:\sdk\samples\Admin>

Konfiguration des ISA Server zur Unterstützung interner Mailclients (z.B. Outlook/Outlook Express)

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

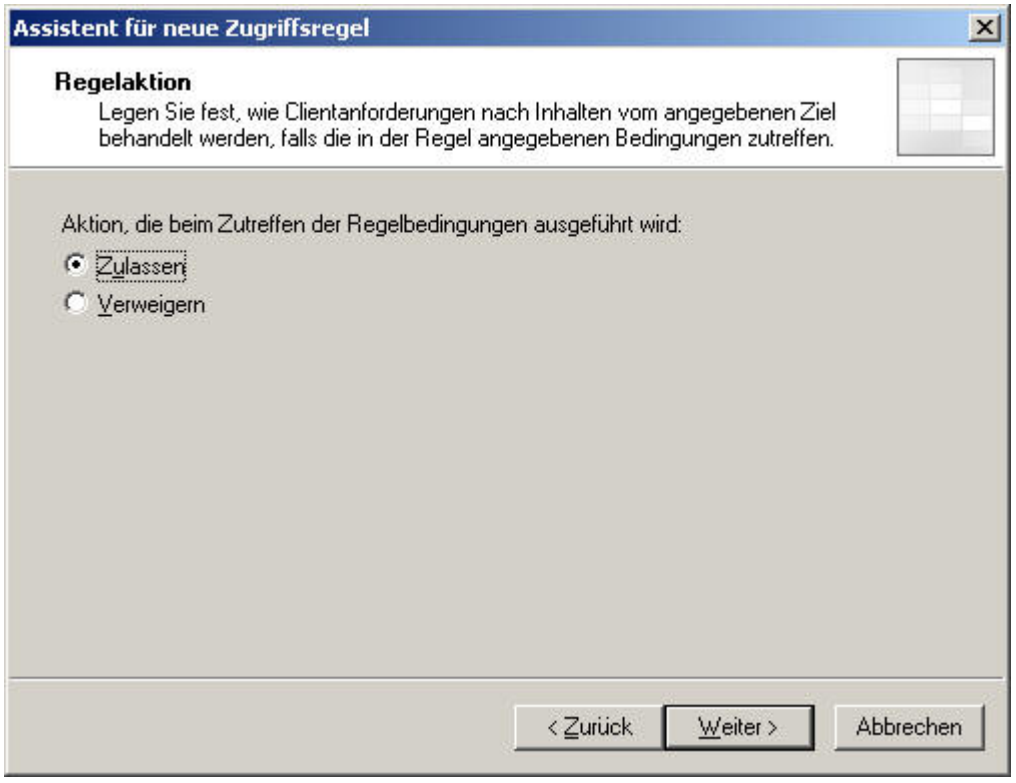
Da im Artikel Erstellen einer Firewallrichtlinie bereits sehr ausführlich auf das Erstellen von Firewallrichtlinien eingegangen wurde, beschränkt sich dieser Artikel auf die wesentlichen Schritte um einem internen Mailclient (wie z.B. Outlook Express) die Anbindung an einen externen Mailserver (z.B. gmx.de) zu ermöglichen.

Nach der ISA Installation sind ja bekanntlich sämtliche Verbindungen blockiert. Jedes notwendige Protokoll muss zuerst zugelassen werden. Damit ein Mailclient mit einem externen Mailserver kommunizieren kann werden gewöhnlich zwei Protokolle benötigt: SMTP fürs senden und POP3 zum Mails abholen. Deshalb sollten auch nur diese beiden Protokolle freigegeben werden. Und das dann am besten nicht gleich für das ganze interne Netzwerk sondern nur für einzeln festgelegte Computer. Warum? Ganz einfach, welchen Grund sollte es z.B. für einen Netzwerkdrucker geben, Mails nach extern versenden zu können?

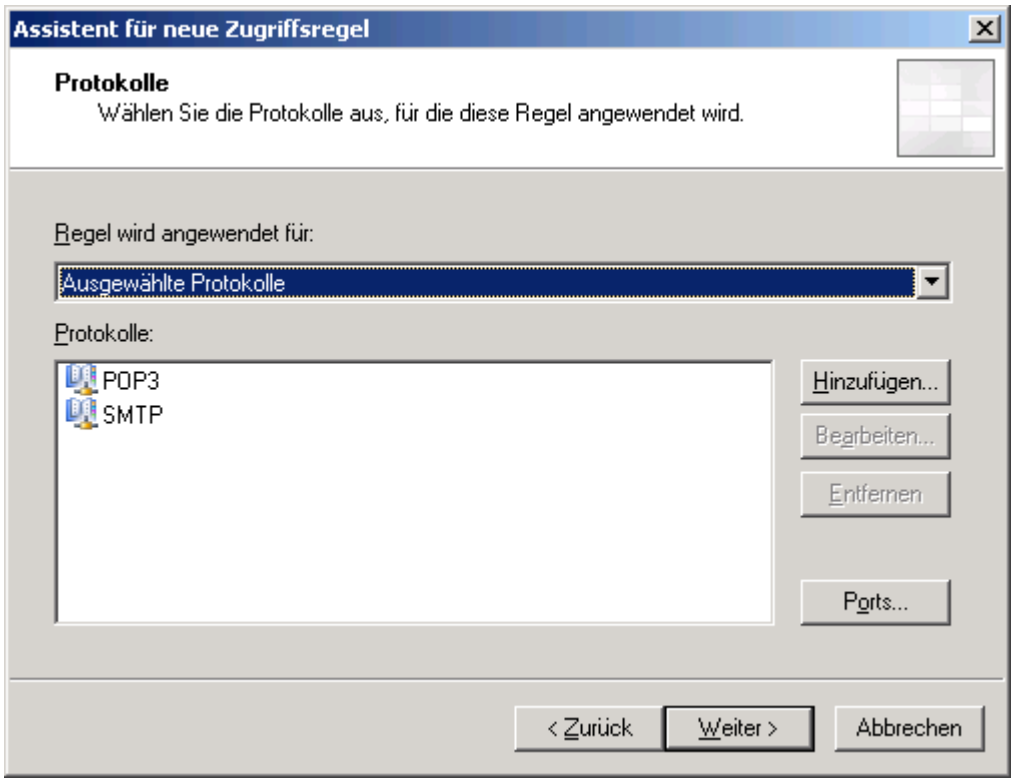
Der ISA Server kann Regeln anhand Benutzernamen oder IP-Adressen zulassen/verweigern. Im ersten Fall ist der Firewallclient notwendig, für IP-basierte Regeln reicht der SecureNAT-Client. Üblicherweise sollte der SecureNAT Client ausreichend sein.

Das folgende Beispiel soll eine Richtlinie erstellen, die folgende Bedingungen erfüllt: Die Benutzer Cornelia, Birgit und Andreas sollen von ihren jeweiligen Clients (192.168.16.19, 192.168.16.59 und 192.168.16.34) ganztags Mails bei GMX abholen und versenden können.

Dazu wird eine neue Firewallrichtlinie erstellt:

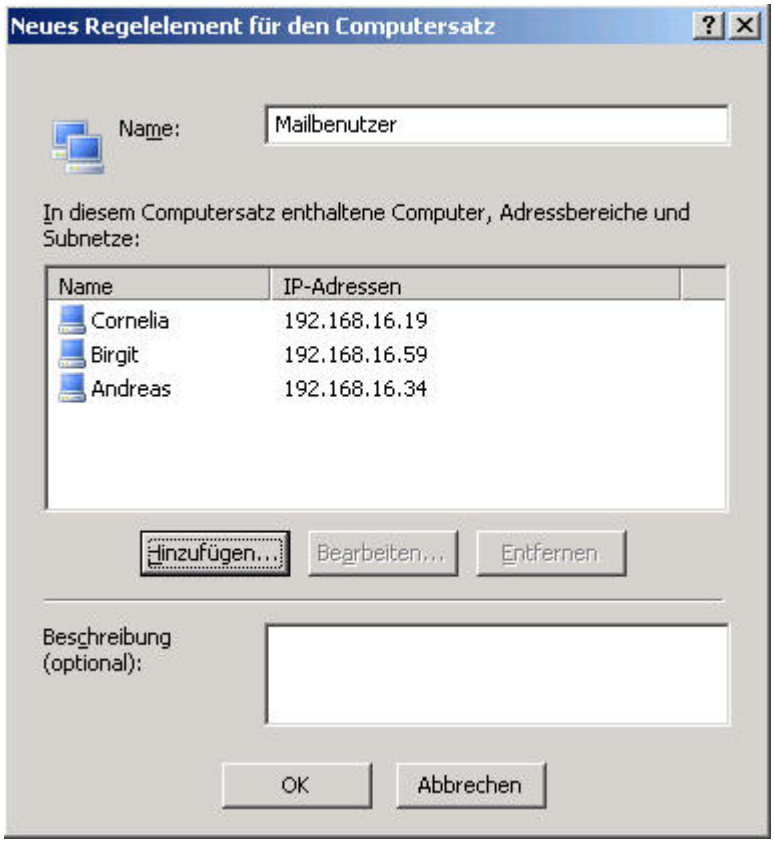


Diese Regel soll eine Zulassungsregel sein...

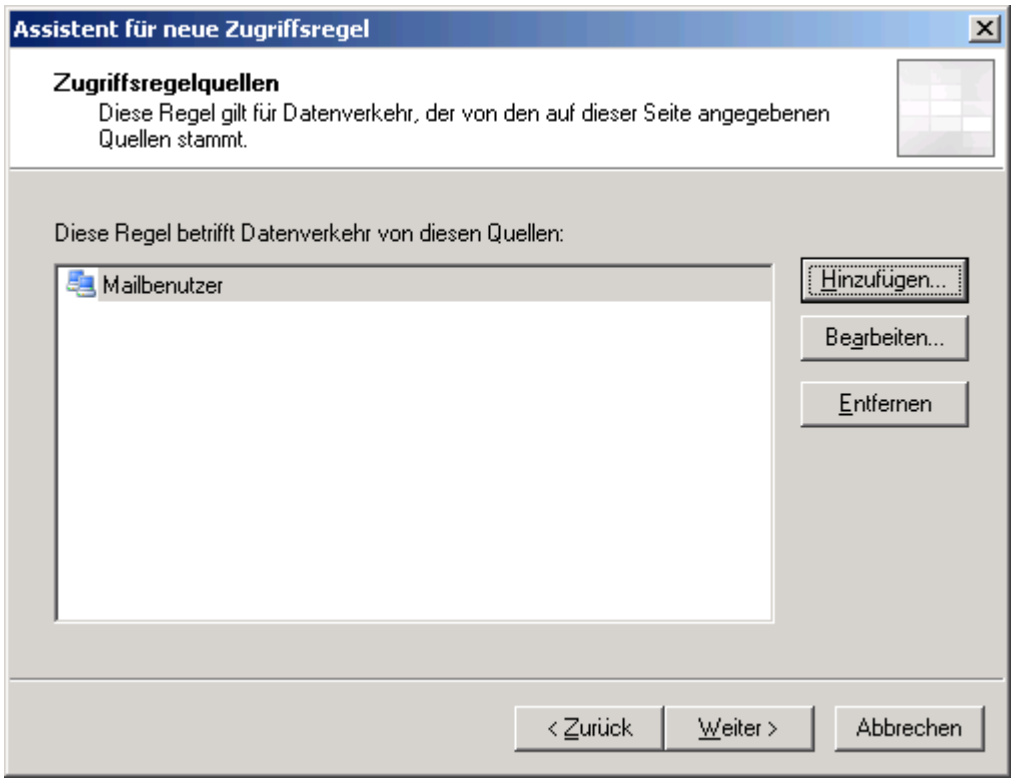


....und nur für POP3 und SMTP gelten.

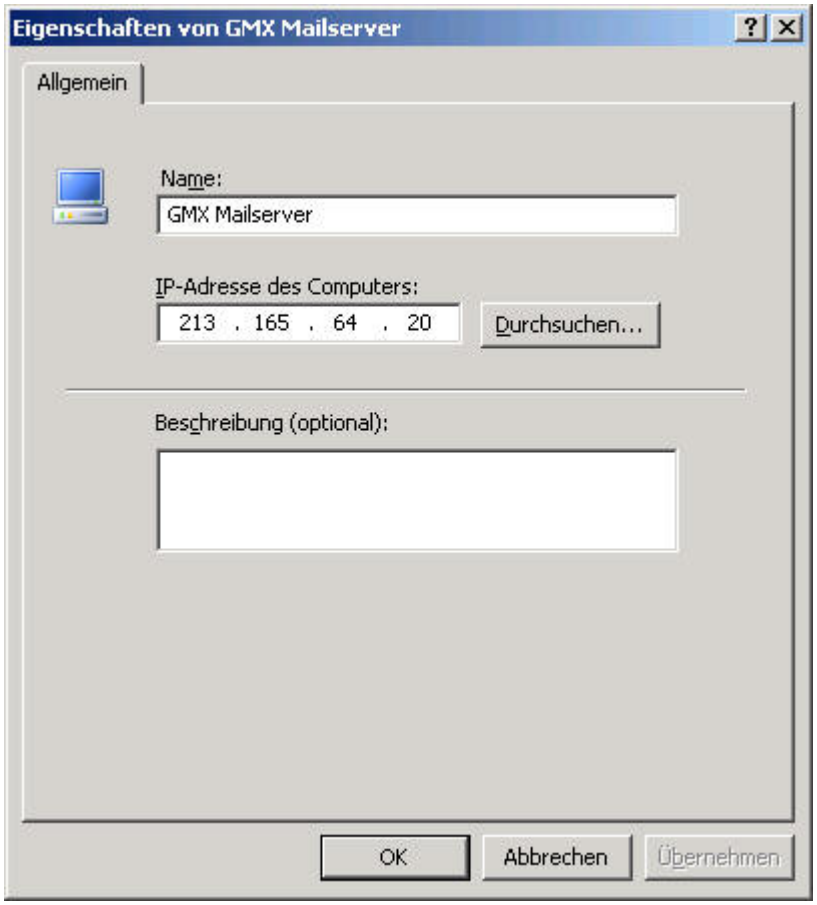
Als nächstes muss ein Computersatz für die drei Benutzer erstellt werden:



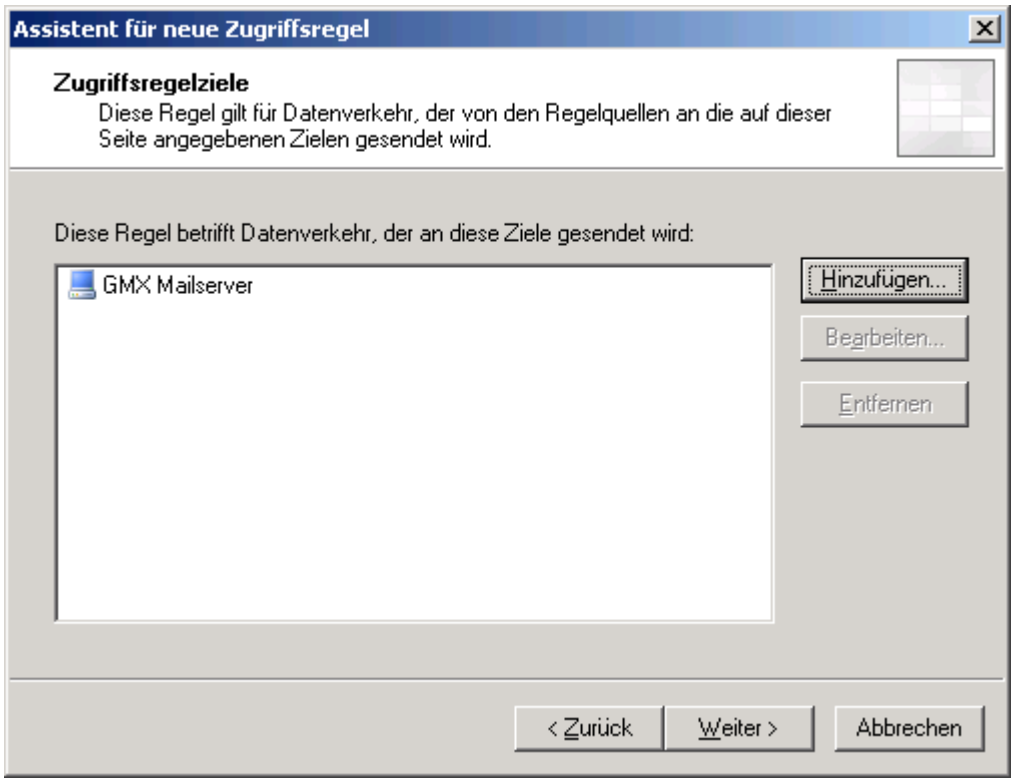
Dieser neu erstellte Computersatz wird als Quelle für die Zulassungsregel verwendet:



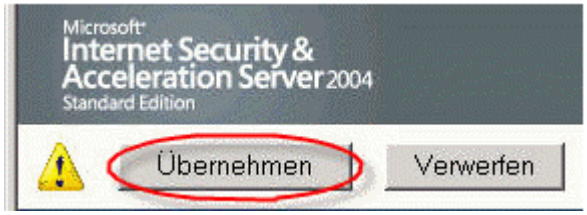
Damit die Benutzer auch nur den erlaubten Mailaccount bei GMX nutzen können wird ein weiteres Computer-Objekt angelegt...

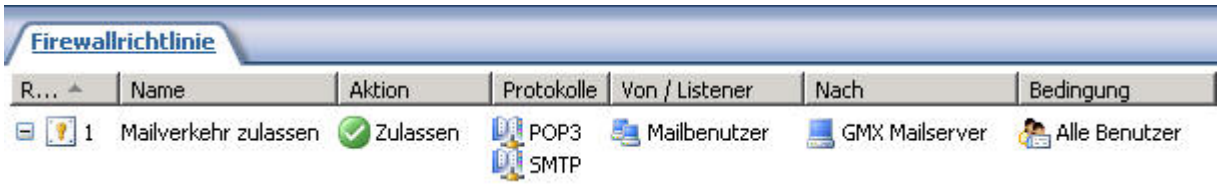


...und als Ziel für die Regel verwendet:



Nachdem der Richtlinienassistent beendet wurde und die neue Regel übernommen wurde ist sie einsatzbereit.





Die berechtigte Frage die hier aufkommen kann ist, warum die drei Benutzer nicht unter Bedingung eingetragen wurden. Die Lösung ist einfach: dazu wäre der Firewallclient notwendig gewesen. Nur mit diesem ist eine echte Benutzerauthentifizierung möglich. In diesem Beispiel sind jedoch nur die IP Adressen der Clients relevant.

Veröffentlichen von Remotedesktop zur Verwaltung des ISA Server Computers

---

Die Informationen in diesem Artikel beziehen sich auf:

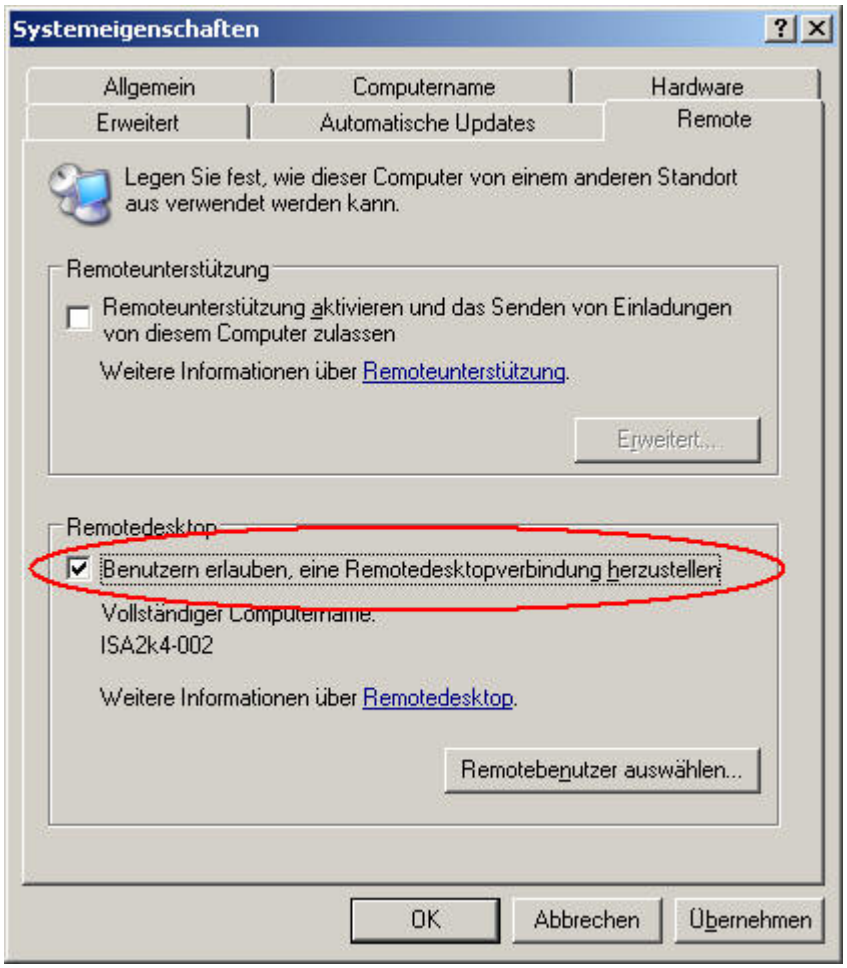
- Microsoft ISA Server 2004

Der unter der Rubrik Administration erschienene Artikel Remoteverwaltung RDP beschreibt die notwendigen und sinnvollen Schritte, wenn von einem internen Client auf den ISA Server Computer per Remotedesktopprotokoll (RDP) zugegriffen werden soll. Dort wurde auch erwähnt, dass diese Konfiguration auch externe Clients berücksichtigen kann. Da dem externen Client durch die Gruppenmitgliedschaft ggfs. zu viele Zugriffsrechte vergeben werden, empfiehlt es sich, eine eigene Firewallrichtlinie für den externen RDP-Zugriff zu erstellen Dies wird im vorliegenden Artikel beschrieben.

Einrichten des ISA Server Computer zur Fernverwaltung mittels Remotedesktop (RDP):

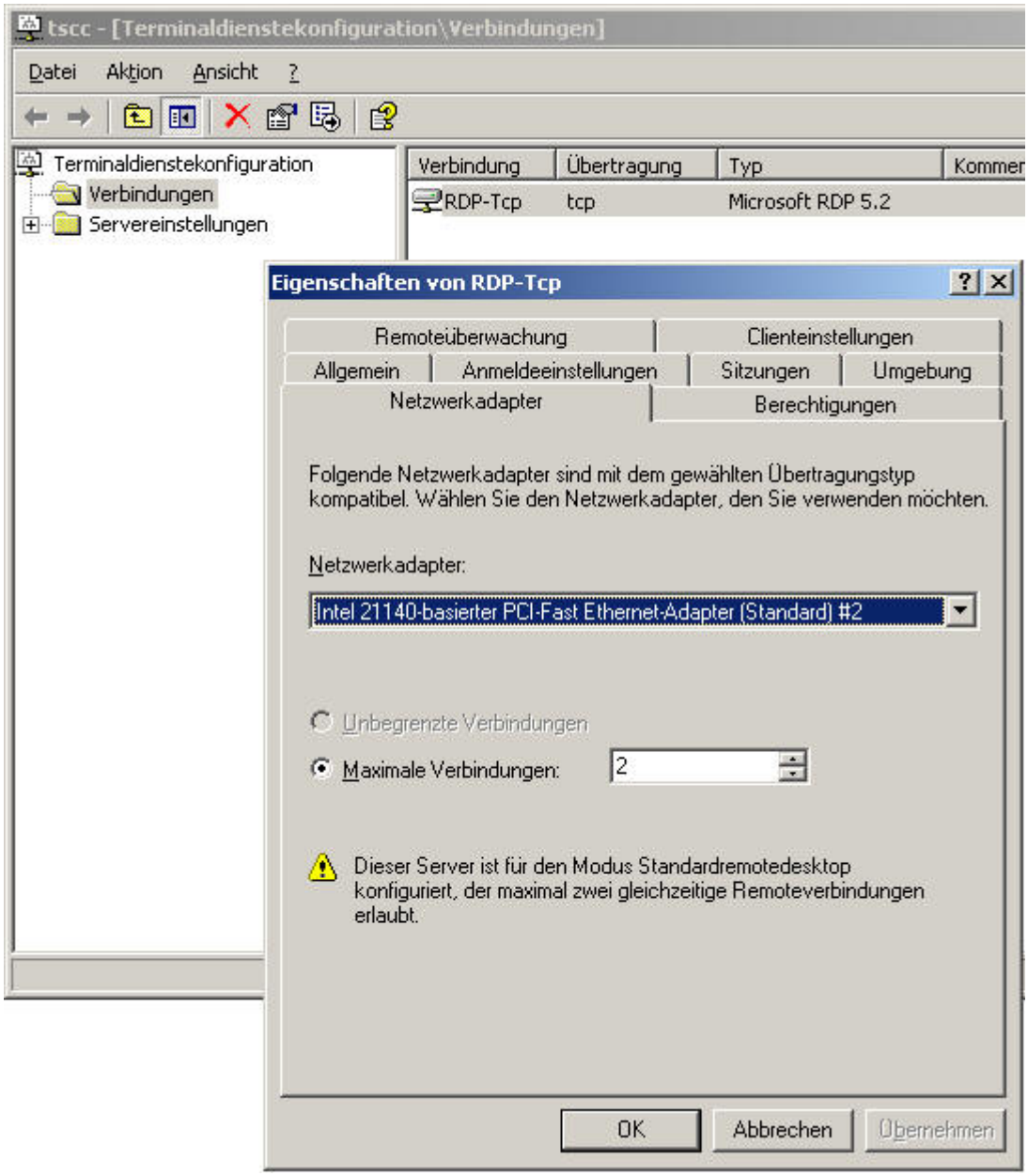
Um den ISA Server über die Remotedesktop-Funktionalität von Windows Server 2003 (bei Windows 2000 Server ist es das selbe Prinzip, die Technik heißt dort jedoch noch "Terminaldienst im Administrationsmodus") verwalten zu können müssen sowohl am Windows Server als auch in der ISA Verwaltung kleine Konfigurationsschritte durchgeführt werden.

Zuerst muss der Windows Server zulassen, dass er über RDP verwaltet werden kann:



In den Systemeigenschaften (Systemsteuerung -> System) muss auf der Registerkarte "Remote" der Remotedesktop aktiviert werden. Standardmäßig dürfen dann nur (lokale) Administrationen eine RDP-Verbindung herstellen. Man kann aber jederzeit weitere berechtigte Benutzer hinzufügen.

Als nächsten Schritt ist es ggfs. sinnvoll, die Terminaldienstekonfiguration anzupassen, dass nur einer der mindestens 2 Netzwerkadapter auf RDP-Anfragen reagiert:



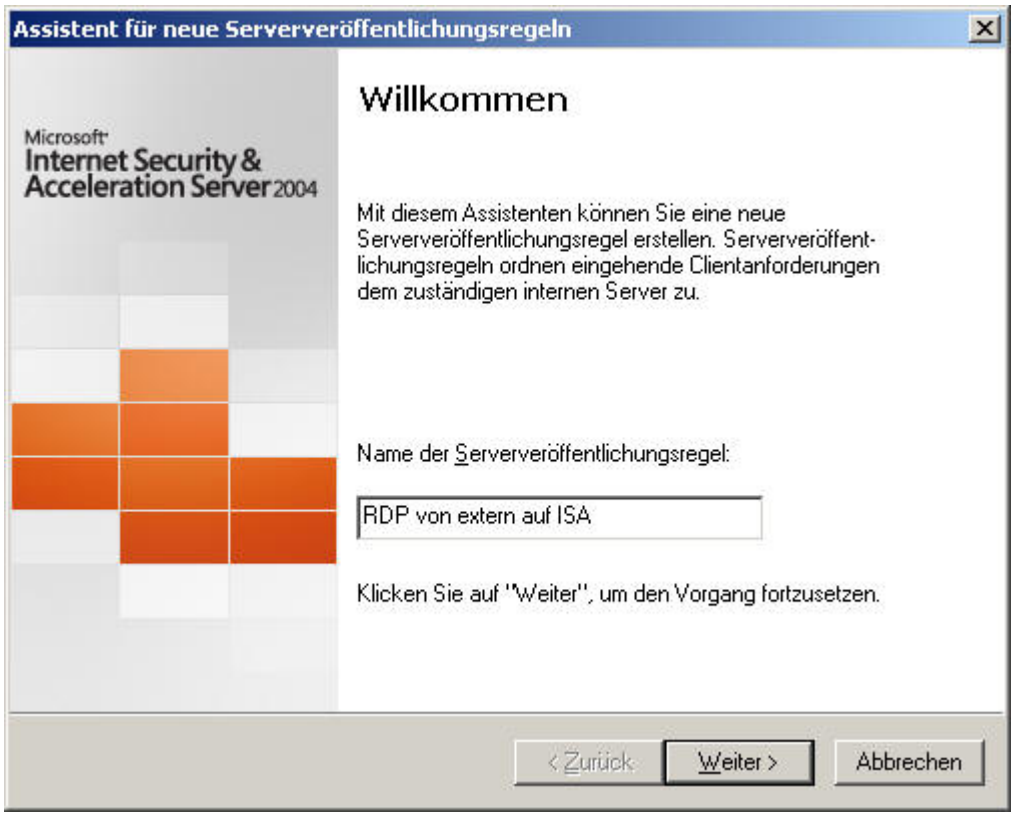
In diesem Beispiel ist die 2. Netzwerkkarte dem internen Netzwerk zugeordnet.

Intern	LAN ...	Aktiviert	Intel 21140-basierter PCI-Fast Ethernet-Adapter (Standard) #2
Extern	LAN ...	Aktiviert	Intel 21140-basierter PCI-Fast Ethernet-Adapter (Standard)

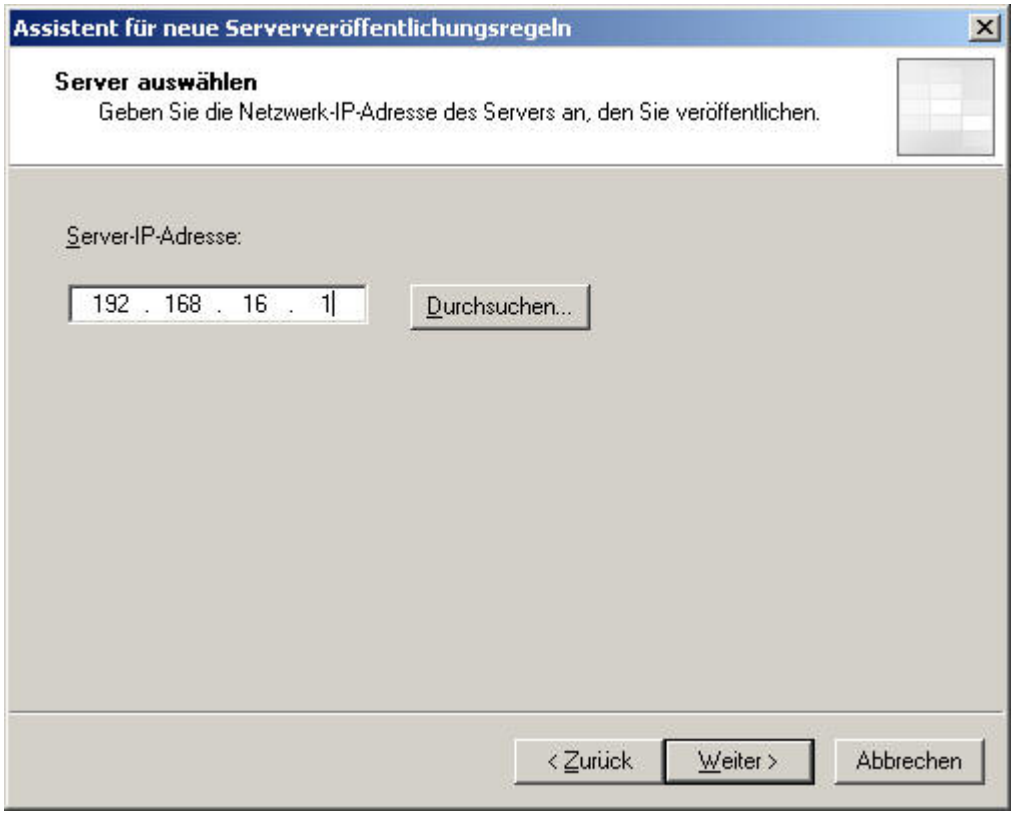
Konfiguration einer Firewallrichtlinie für externen RDP-Zugriff

Nachdem die Windows-seitigen Einstellungen vorgenommen wurden, kann eine Firewallrichtlinie erstellt werden.

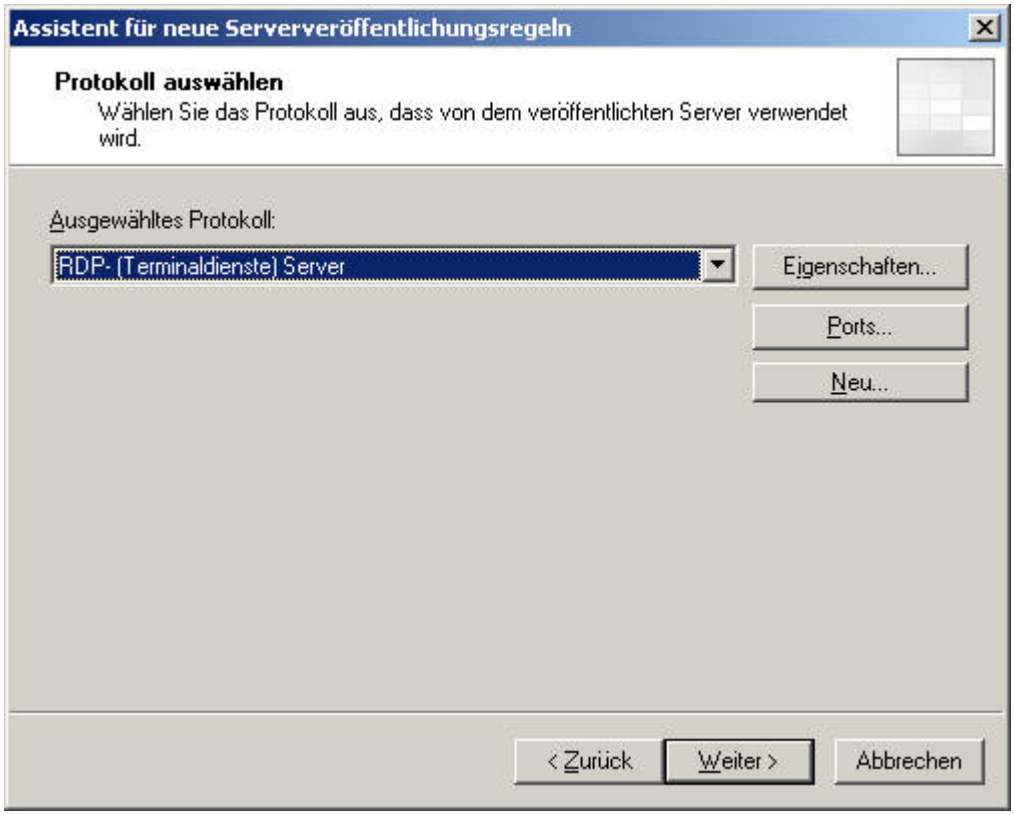
Erstellen Sie eine neue Serververöffentlichungsregel:



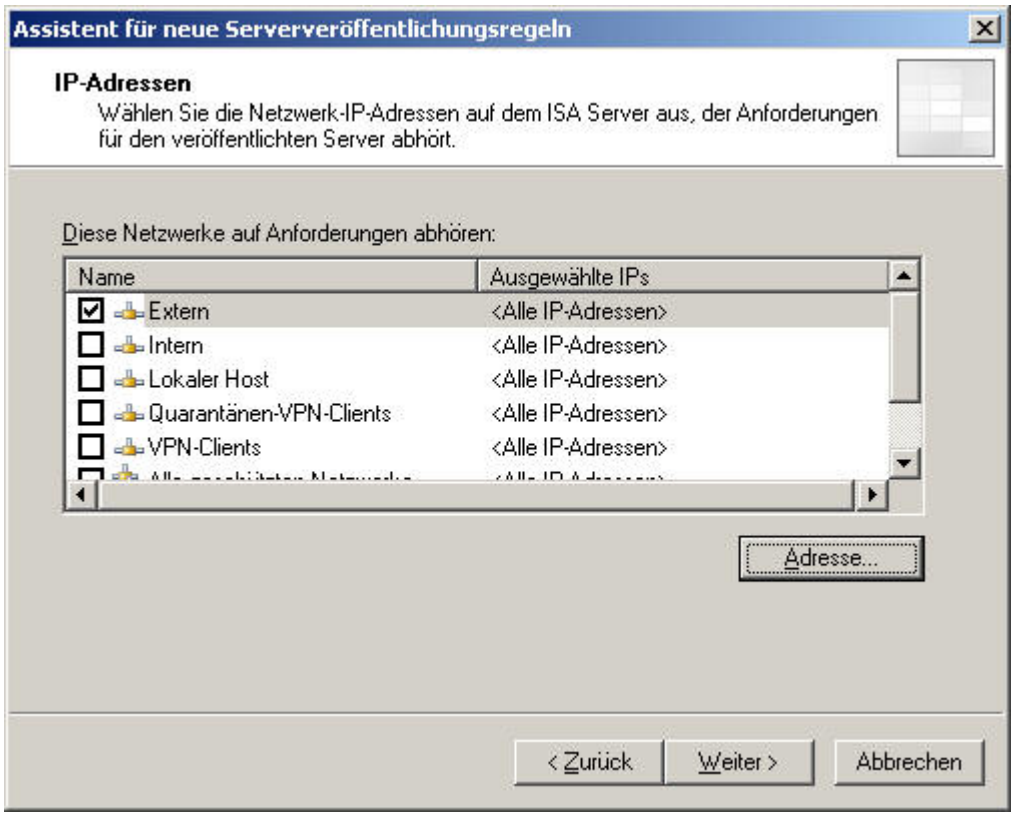
Geben Sie die interne IP Adresse des ISA Server Computers an:



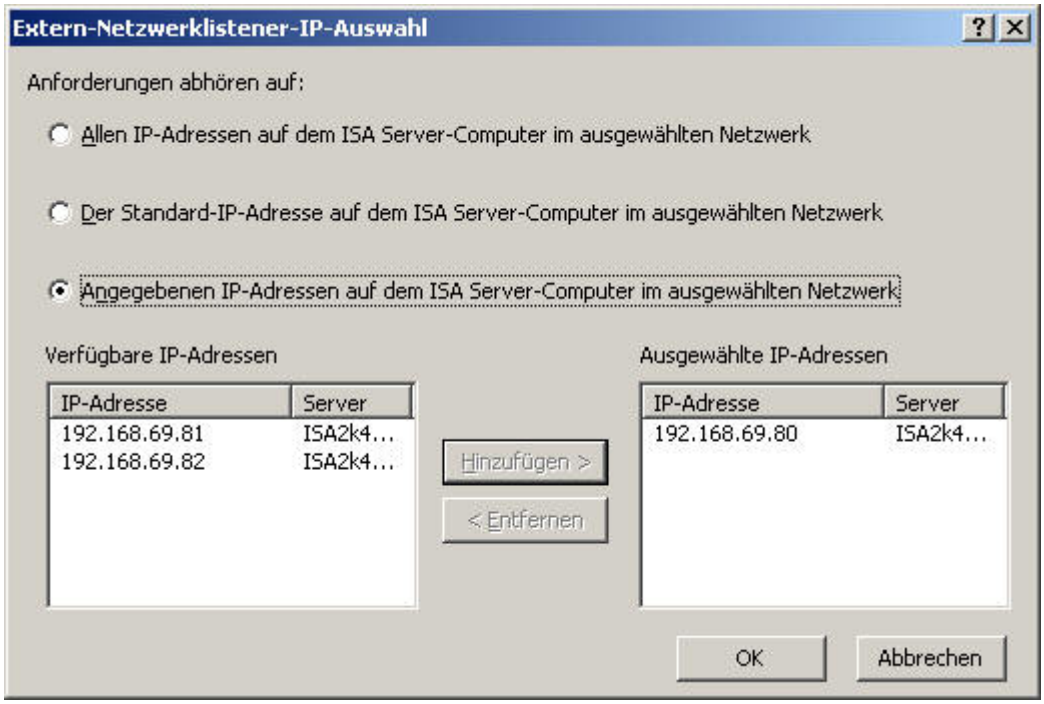
Wählen Sie das RDP-Server-Protokoll aus:

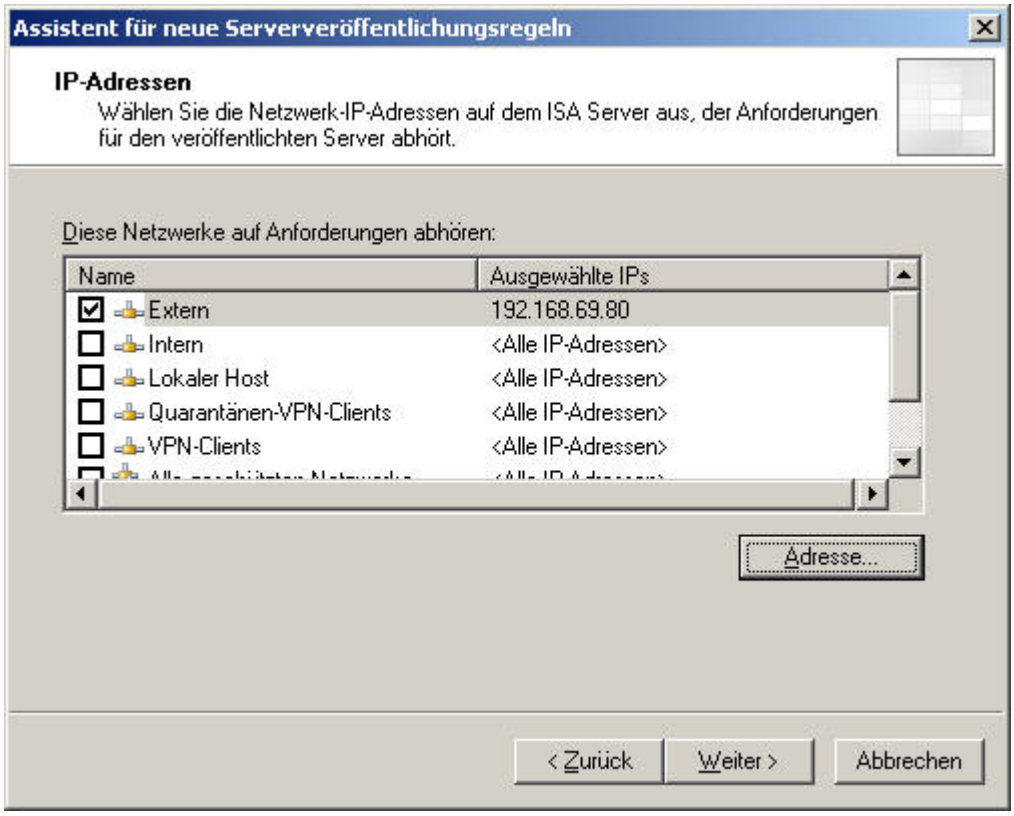


Legen Sie anschließend das Netzwerk aus, von welchem die Anfragen kommen.

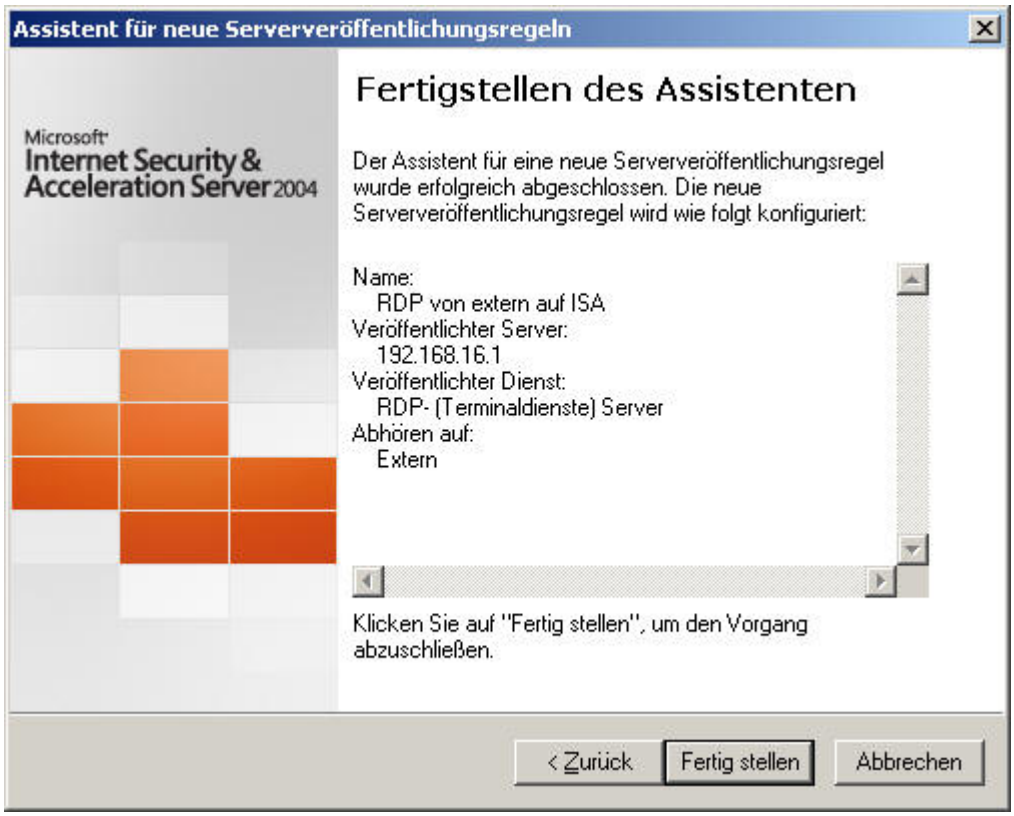


Hinweis: Sollte der ISA Server über mehrere externe IP-Adressen verfügen, können Sie mittels "Adresse..." festlegen, auf welcher IP-Adresse RDP-Anfragen entgegengenommen werden:

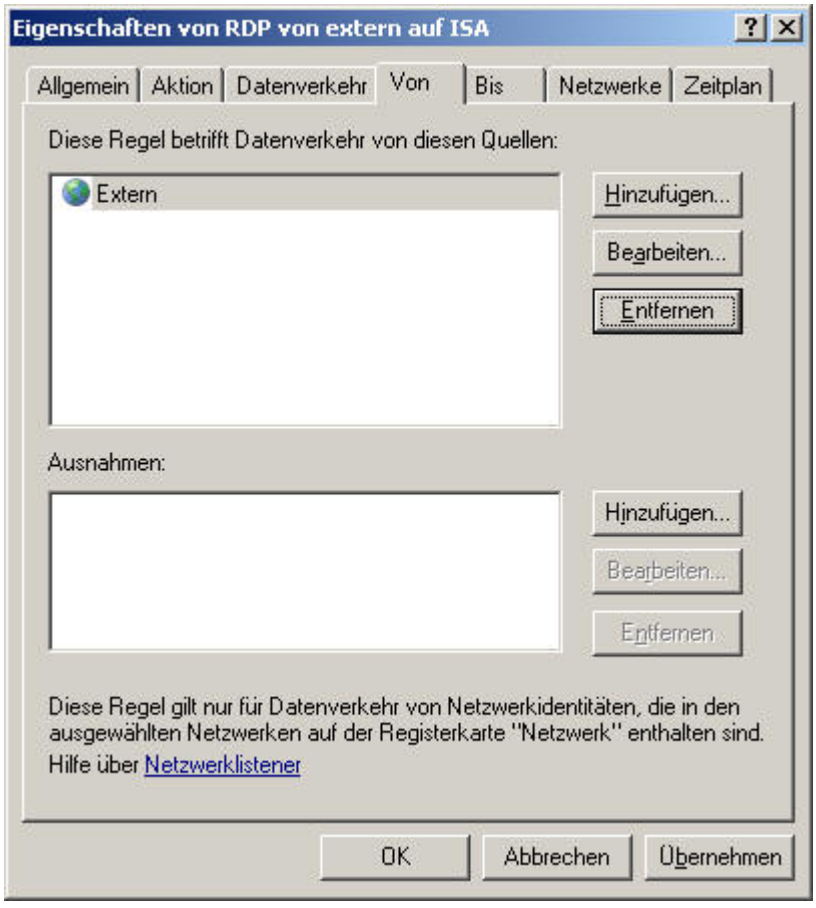




Die letzte Seite des Assistenten zeigt wie immer eine Übersicht an.



Bevor die neu erstelle Firewallrichtlinie übernommen wird, sollten Sie noch eine kleine Korrektur in den Eigenschaften der Richtlinie vornehmen. Gehen Sie dazu auf die Registerkarte "Von".



Standardmäßig wird als Quellnetzwerk "beliebig" ausgewählt. Ändern Sie das in "Extern" ab. Sollten Sie noch weitere Einschränkungen vornehmen wollen, so tun Sie es hier und jetzt. Es ist z.B. denkbar, dass Sie nur bestimmte vordefinierte Computer in einem Computersatz zusammenfassen und nur diesen den Zugriff auf diese Regel erlauben. Dann würden Sie natürlich diesen Computersatz statt "Extern" hinzufügen.

Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

Veröffentlichen eines internen Terminalserver oder interner Remotedesktop Services

---

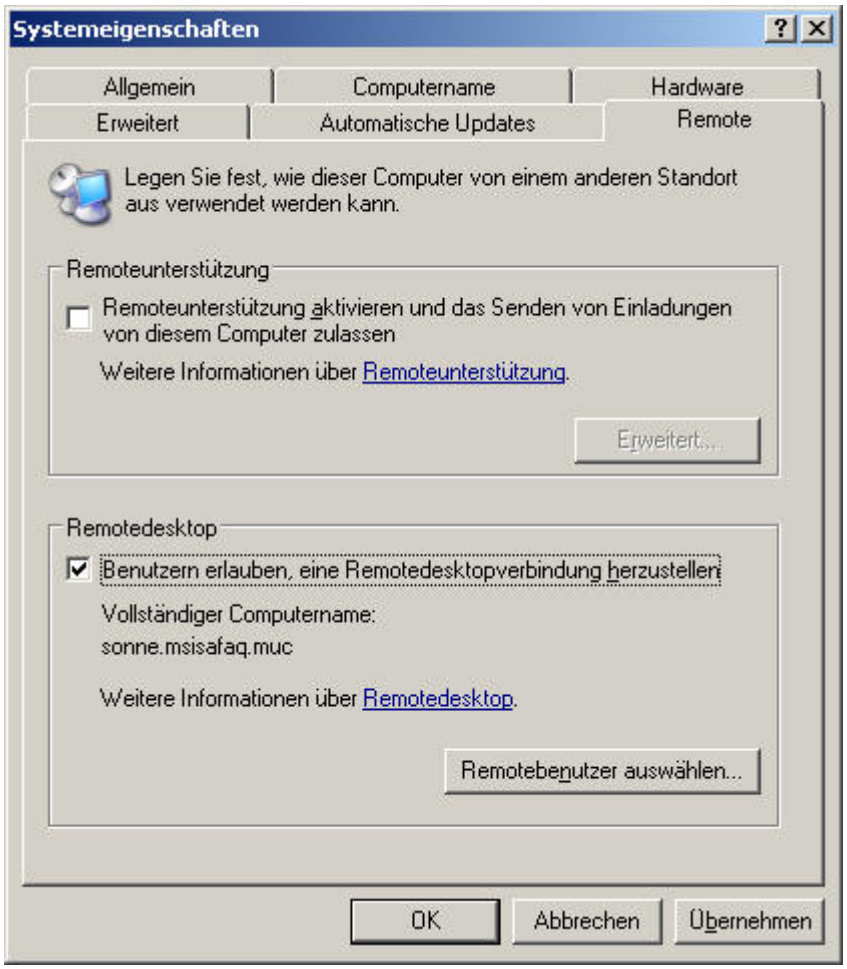
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Der vorliegende Artikel beschreibt die notwendigen Schritte, um den ISA Server für den Zugriff über das Remotedesktopprotokoll (RDP) auf einen internen Server einzurichten.

Einrichten des internen Servers oder Computer zur Fernverwaltung mittels Remotedesktop (RDP):

Um den Server über die Remotedesktop-Funktionalität von Windows Server 2003 (bei Windows 2000 Server ist es das selbe Prinzip, die Technik heißt dort jedoch noch "Terminaldienst im Administrationsmodus") verwalten zu können muss am Windows Server ein kleiner Konfigurationsschritt durchgeführt werden.



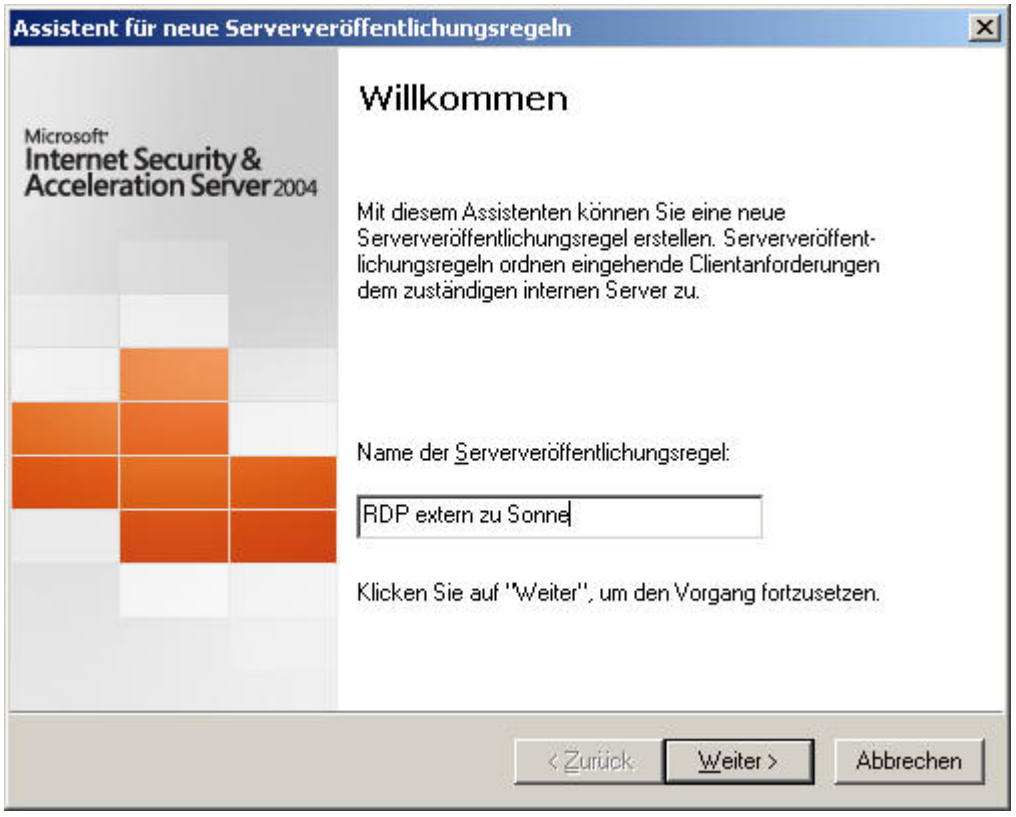
In den Systemeigenschaften (Systemsteuerung -> System) muss auf der Registerkarte "Remote" der Remotedesktop aktiviert werden. Standardmäßig dürfen dann nur (lokale) Administrationen eine RDP-Verbindung herstellen. Man kann aber jederzeit weitere berechtigte Benutzer hinzufügen.

Sollten Sie die "echten" Terminaldienste veröffentlichen wollen, ist dieser Schritt ggfs. nicht notwendig.

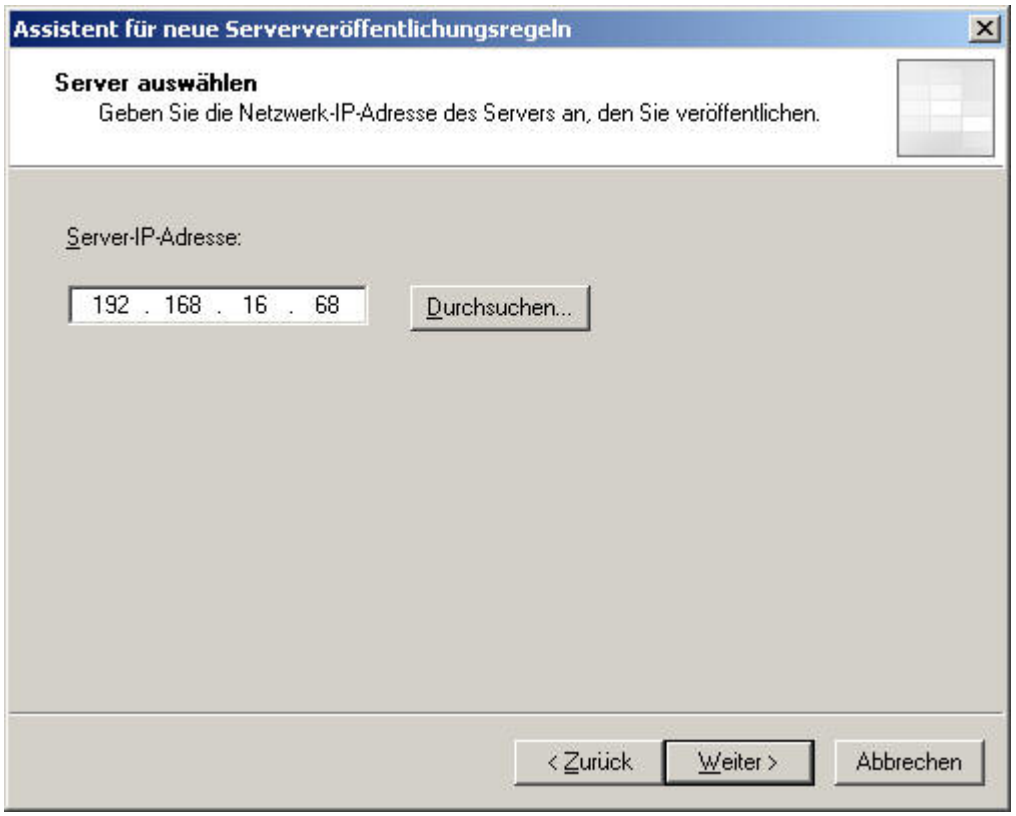
Konfiguration einer Firewallrichtlinie für externen RDP-Zugriff

Nachdem die Windows-seitigen Einstellungen vorgenommen wurden, kann eine Firewallrichtlinie erstellt werden.

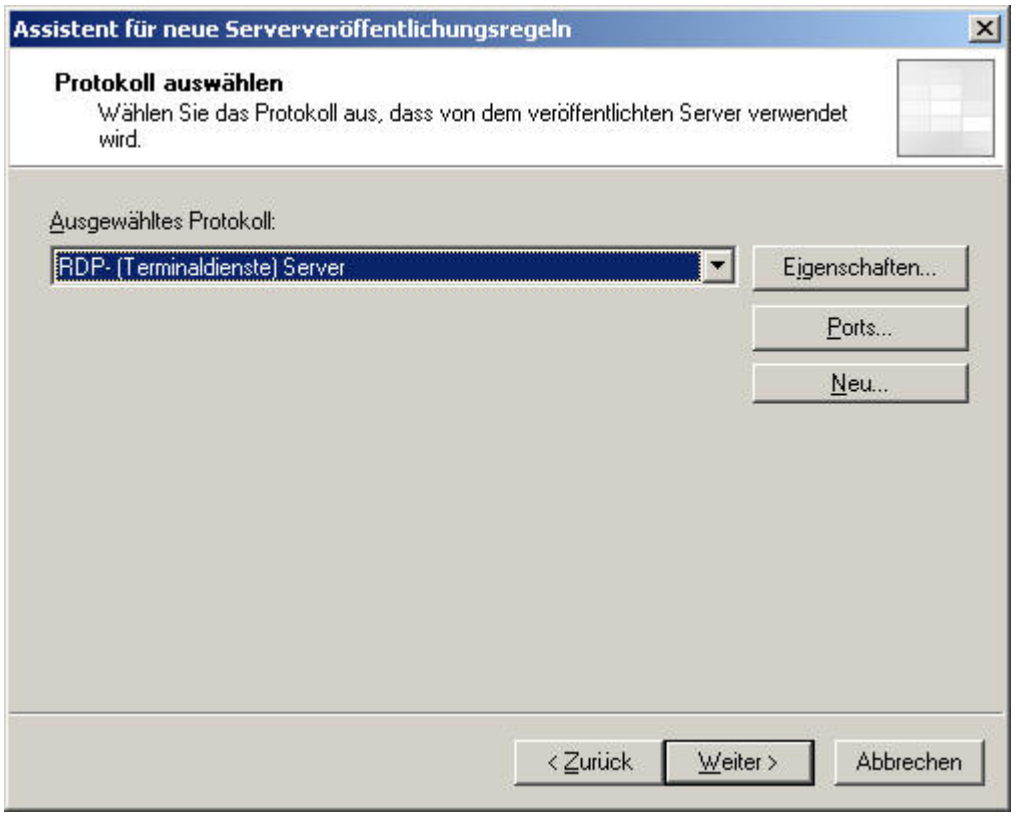
Erstellen Sie eine neue Serververöffentlichungsregel:



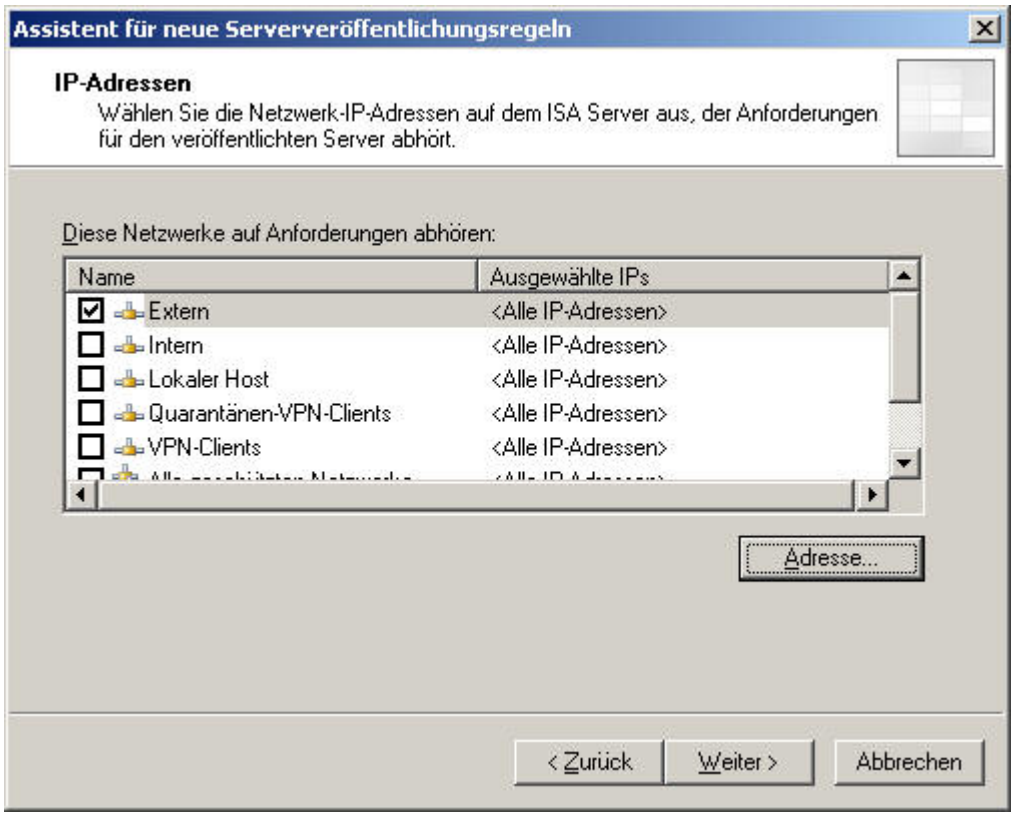
In diesem Beispiel heißt der interne Server "Sonne" und hat die IP-Adresse 192.168.16.68.



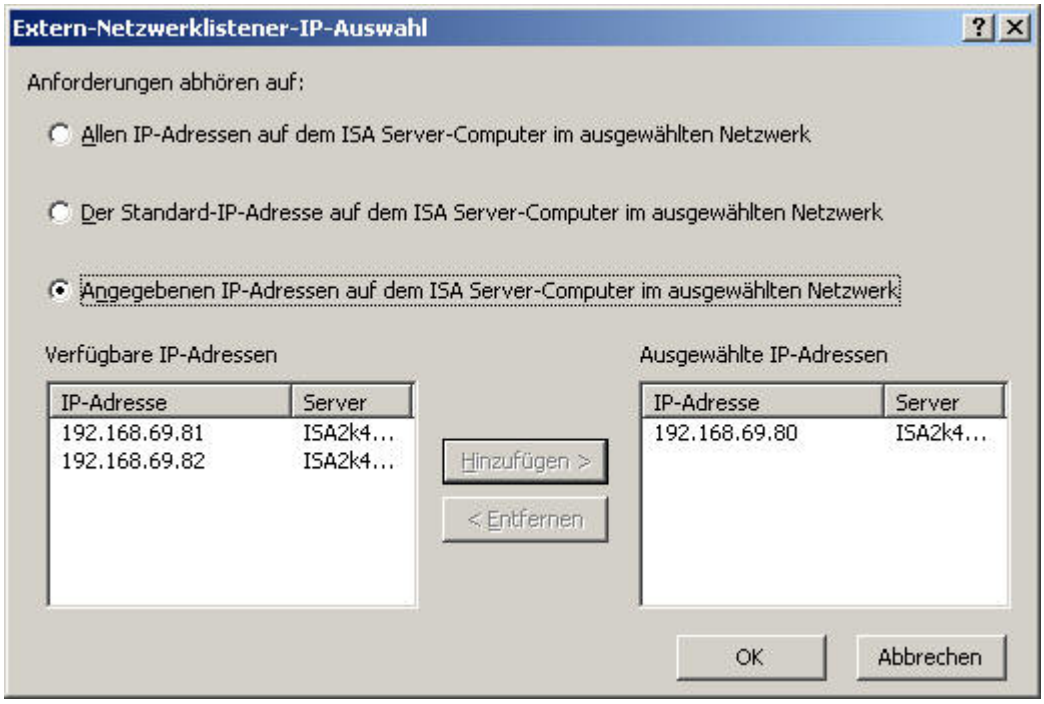
Wählen Sie das RDP-Server-Protokoll aus:

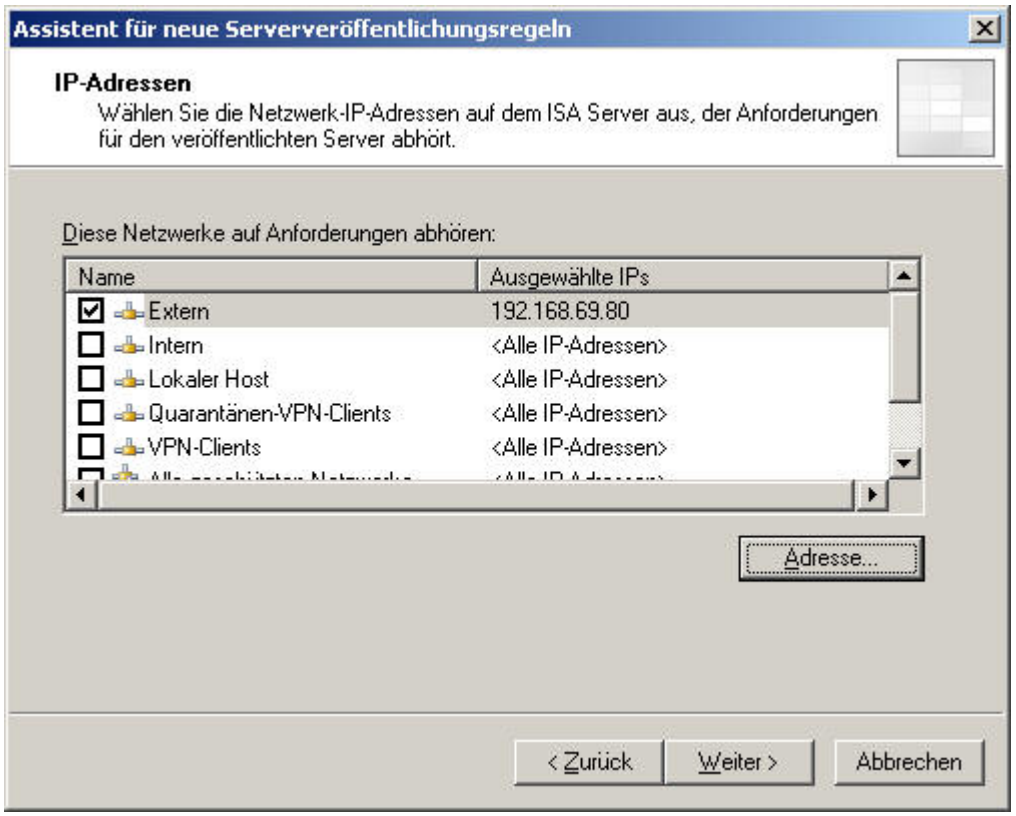


Legen Sie anschließend das Netzwerk aus, von welchem die Anfragen kommen.



Hinweis: Sollte der ISA Server über mehrere externe IP-Adressen verfügen, können Sie mittels "Adresse..." festlegen, auf welcher IP-Adresse RDP-Anfragen entgegengenommen werden:

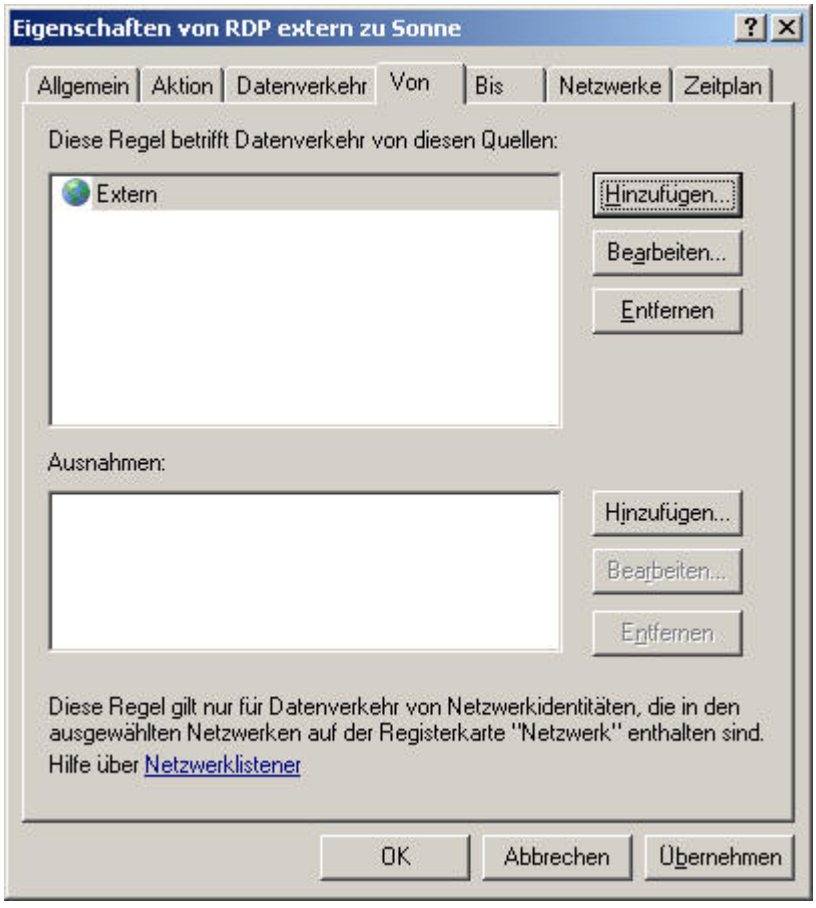




Hinweis: Sollten Sie mehrere interne Server (oder den ISA Server Computer) gleichzeitig per RDP von extern zugänglich machen, müssen Sie dafür unterschiedliche externe IP-Adressen oder ein alternativer Port verwenden. Sie können mit einer externen IP Adresse maximal einen internen Server veröffentlichen.

Die letzte Seite des Assistenten zeigt wie immer eine Übersicht an.

Bevor die neu erstelle Firewallrichtlinie übernommen wird, sollten Sie noch eine kleine Korrektur in den Eigenschaften der Richtlinie vornehmen. Gehen Sie dazu auf die Registerkarte "Von".



Standardmäßig wird als Quellnetzwerk "beliebig" ausgewählt. Ändern Sie das in "Extern" ab. Sollten Sie noch weitere Einschränkungen vornehmen wollen, so tun Sie es hier und jetzt. Es ist z.B. denkbar, dass Sie nur bestimmte vordefinierte Computer in einem Computersatz zusammenfassen und nur diesen den Zugriff auf diese Regel erlauben. Dann würden Sie natürlich diesen Computersatz statt "Extern" hinzufügen.

Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

Veröffentlichen eines internen Terminalserver oder interner Remotedesktop Services auf einem alternativen Port

---

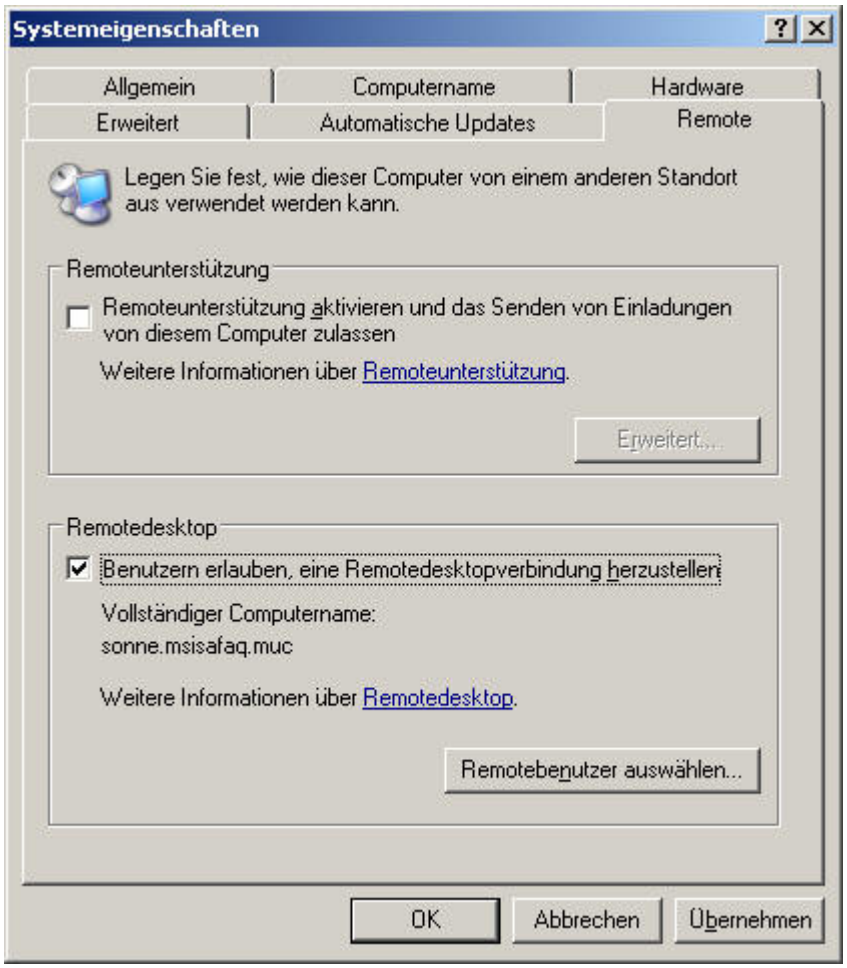
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Der vorliegende Artikel beschreibt als Ergänzung zum Artikel RDP-Serververöffentlichung die notwendigen Schritte, um einen internen Computer mittels des Remotedesktopprotokolls auf einem alternativen (nicht-standard) Port zu veröffentlichen. Ein alternativer Port ist dann notwendig oder sinnvoll, wenn entweder mehrere Server über lediglich eine extern vorhandene IP Adresse veröffentlicht werden soll oder wenn das Sicherheitskonzept die Nutzung von nicht-standard Ports vorsieht.

Einrichten des internen Servers oder Computer zur Fernverwaltung mittels Remotedesktop (RDP):

Um den Server über die Remotedesktop-Funktionalität von Windows Server 2003 (bei Windows 2000 Server ist es das selbe Prinzip, die Technik heißt dort jedoch noch "Terminaldienst im Administrationsmodus") verwalten zu können muss am Windows Server ein kleiner Konfigurationsschritt durchgeführt werden.



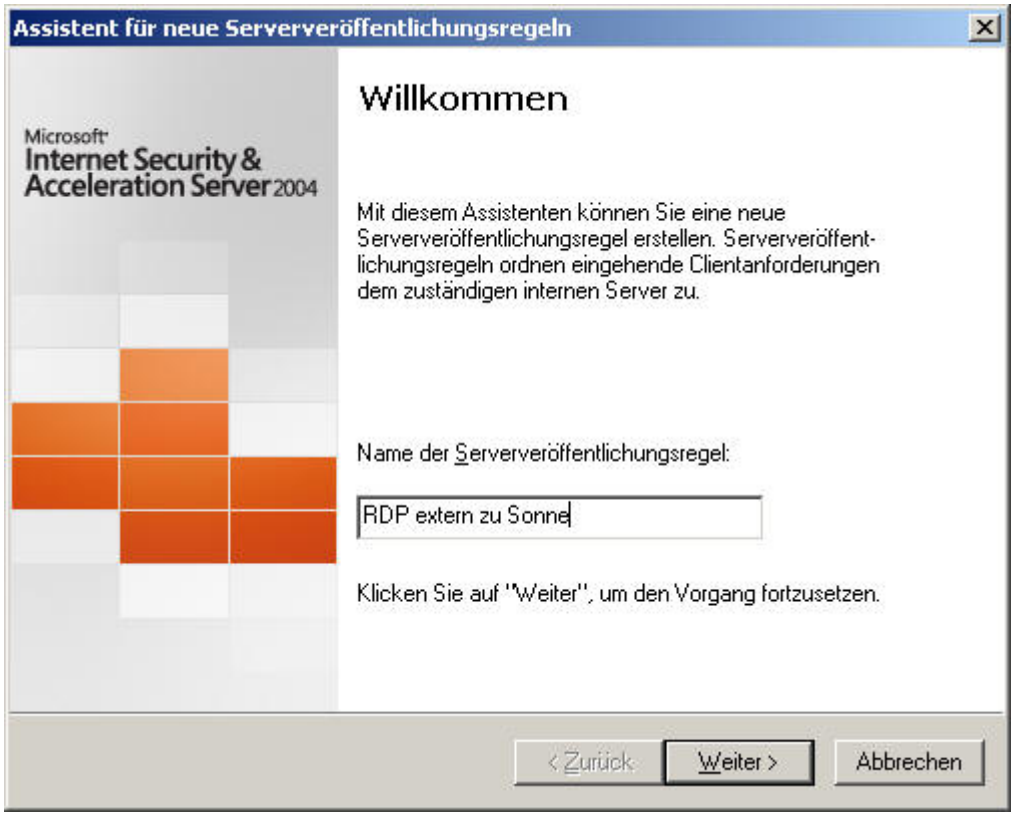
In den Systemeigenschaften (Systemsteuerung -> System) muss auf der Registerkarte "Remote" der Remotedesktop aktiviert werden. Standardmäßig dürfen dann nur (lokale) Administrationen eine RDP-Verbindung herstellen. Man kann aber jederzeit weitere berechtigte Benutzer hinzufügen.

Sollten Sie die "echten" Terminaldienste veröffentlichen wollen, ist dieser Schritt ggfs. nicht notwendig.

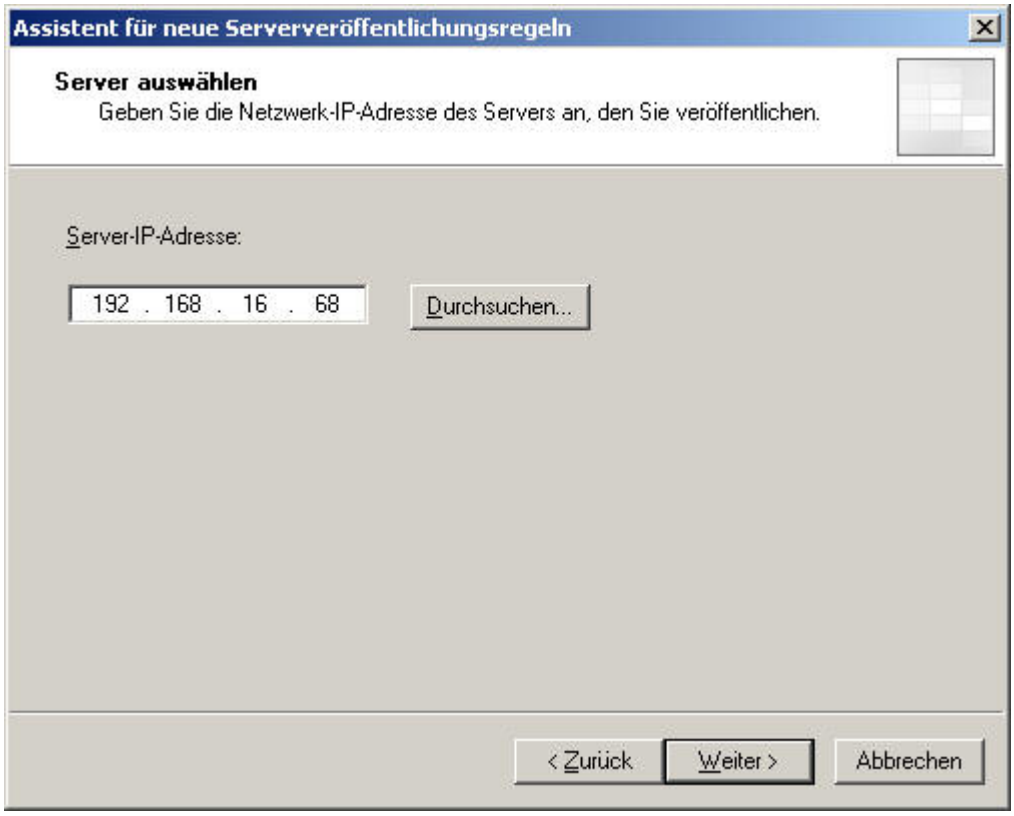
Konfiguration einer Firewallrichtlinie für externen RDP-Zugriff

Nachdem die Windows-seitigen Einstellungen vorgenommen wurden, kann eine Firewallrichtlinie erstellt werden.

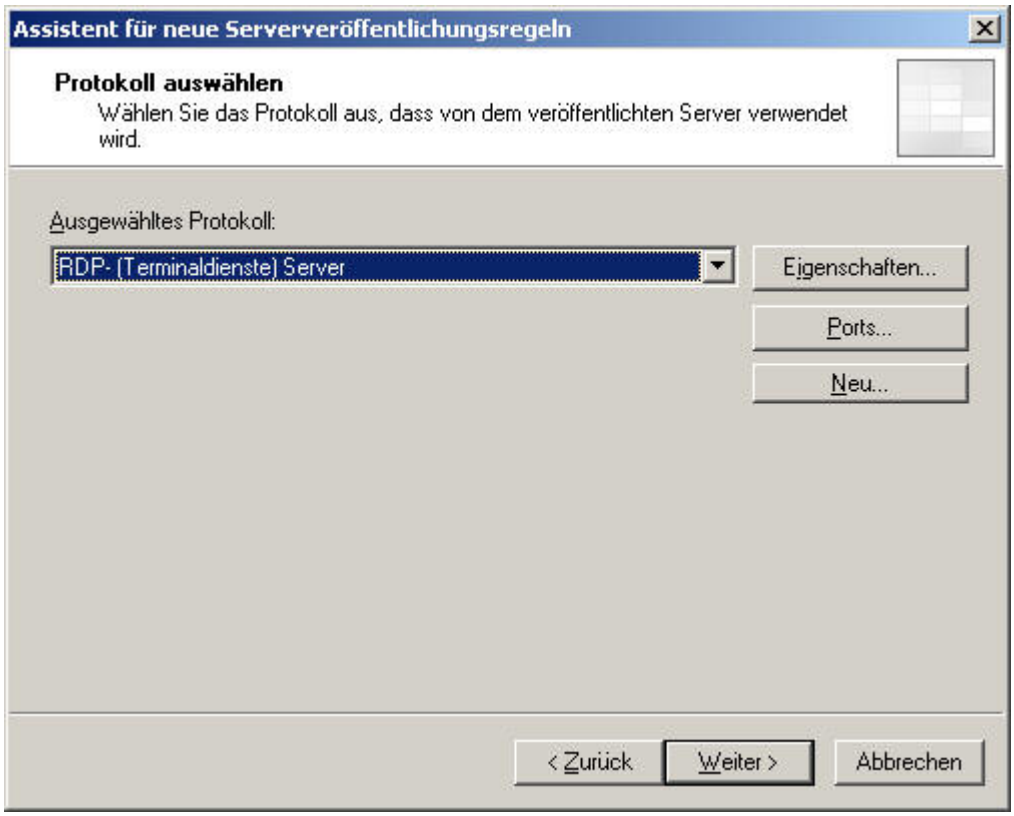
Erstellen Sie eine neue Serververöffentlichungsregel:



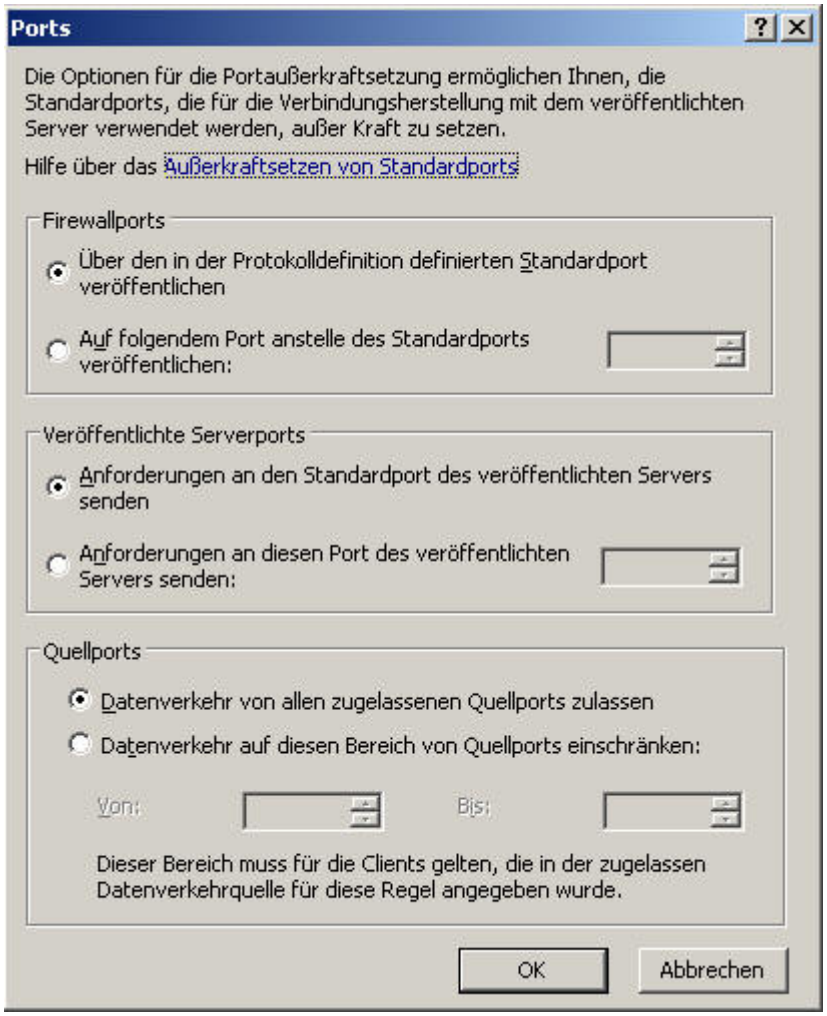
In diesem Beispiel heißt der interne Server "Sonne" und hat die IP-Adresse 192.168.16.68.



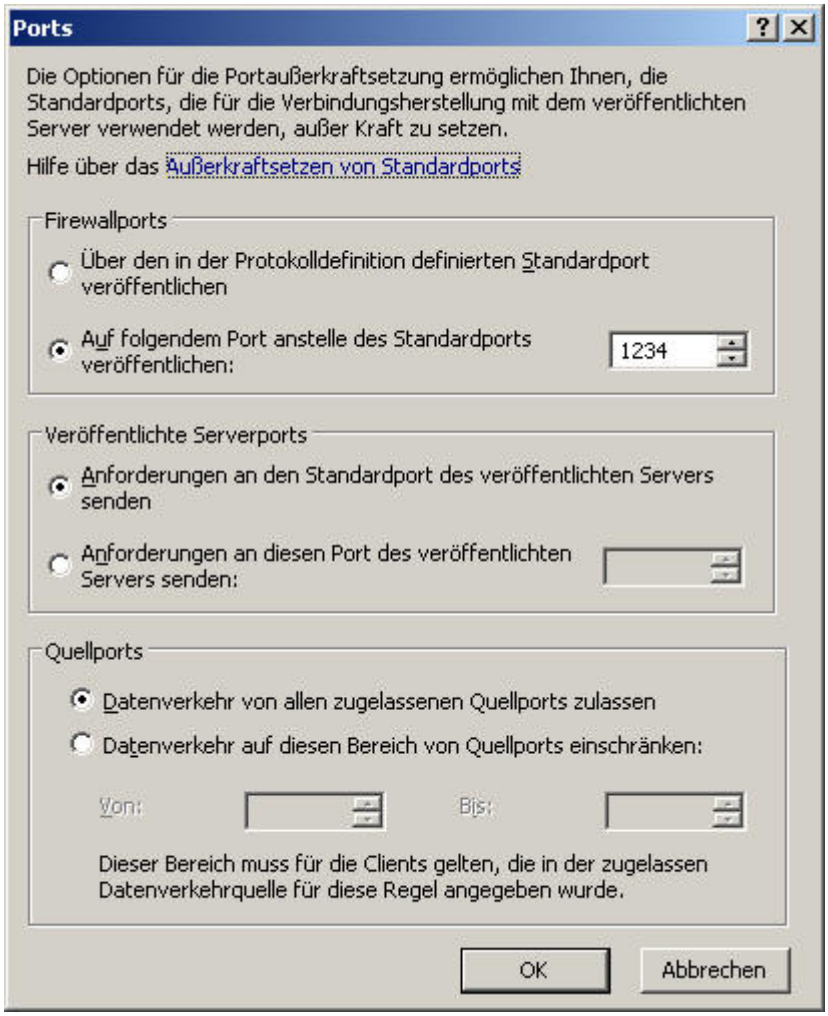
Wählen Sie das RDP-Server-Protokoll aus:



Über die Schaltfläche "Ports" gelangen Sie in den Konfigurationsbereich für den alternativen Port.

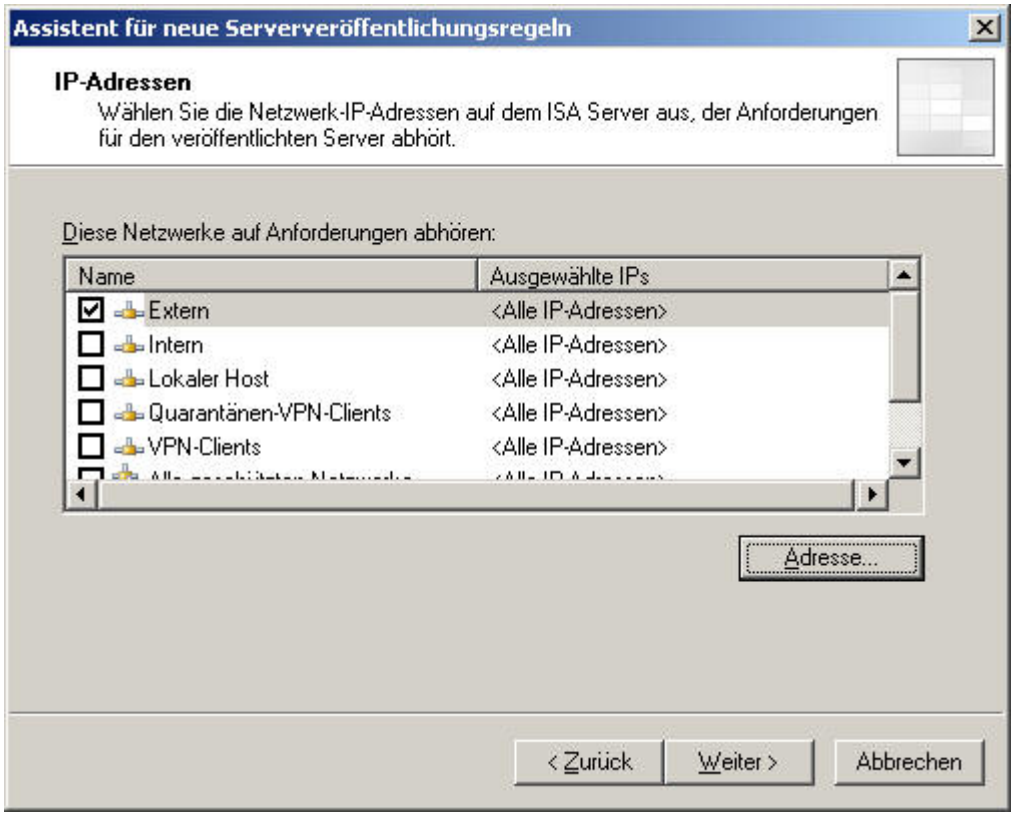


Dabei ist für das hier besprochene Szenario lediglich der oberste Abschnitt "Firewallports" interessant. Durch die Option "Auf folgendem Port anstelle des Standardports veröffentlichen" können Sie einen alternativen Port wie z.B. 1234 statt des üblichen Ports 3389 verwenden. Externe Clients müssen dann in ihrer Remotedesktopverbindung (siehe unten) den alternativen Port angeben.

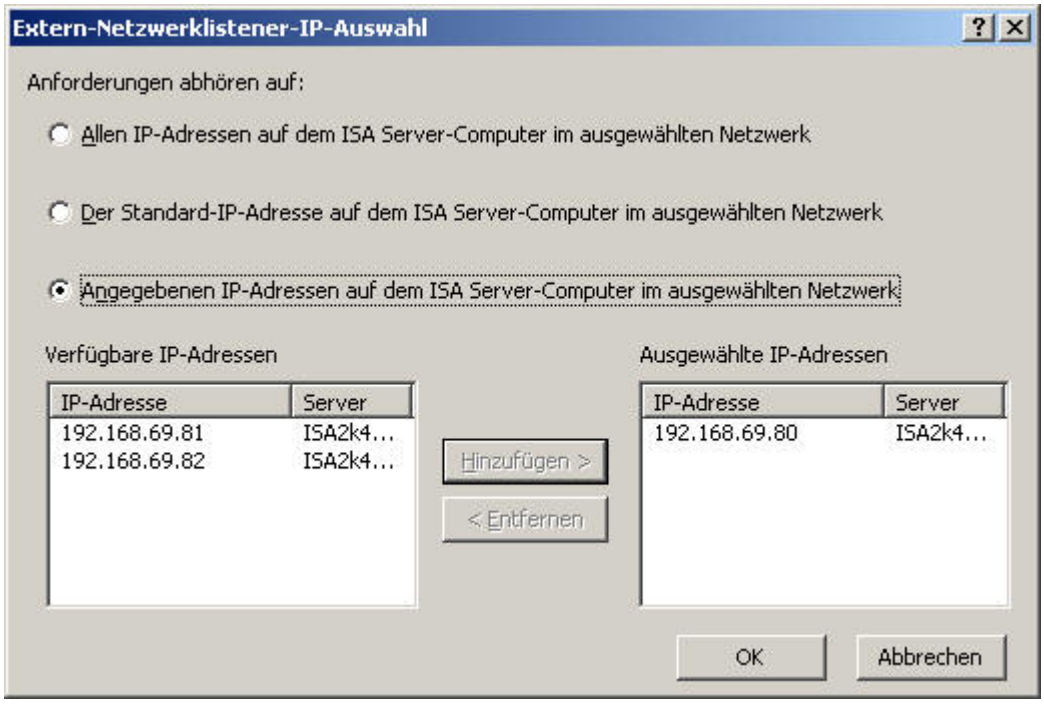


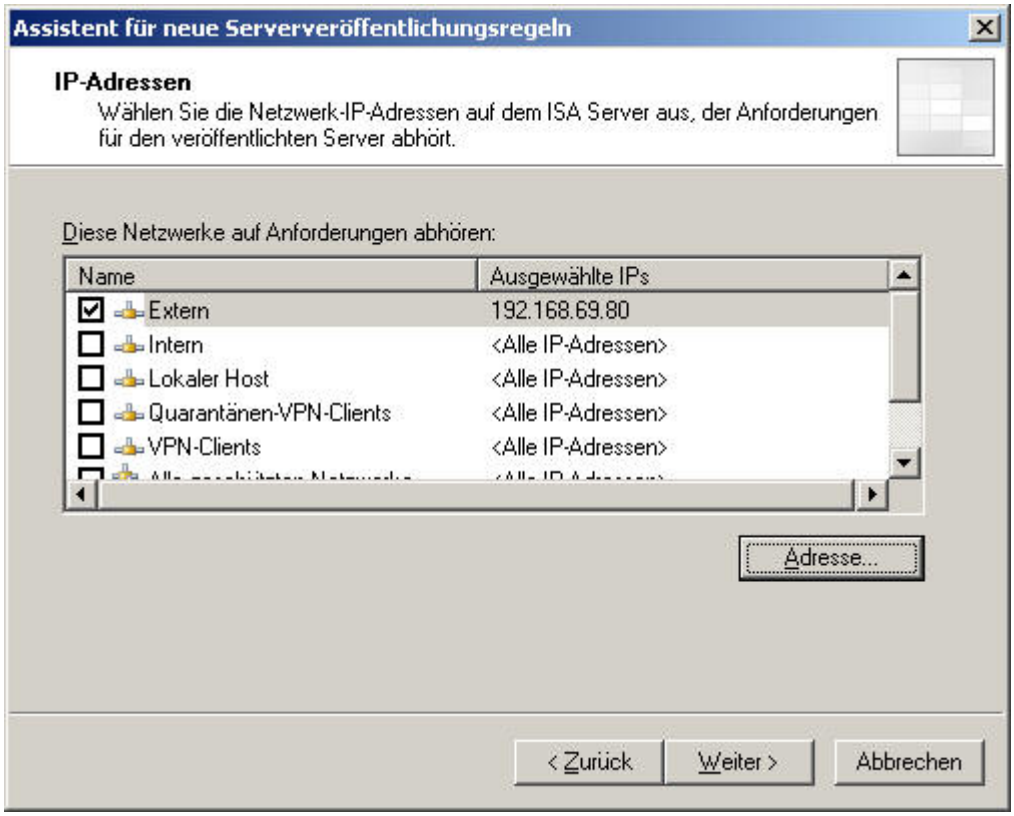
Mittels der mittleren Option "Veröffentlichte Serverports" können Sie z.B. den ISA Server auf Port 3389 abhören lassen, die Verbindung dann jedoch an den internen Terminalserver auf Port 1234 weiterleiten. Dies könnte dann notwendig sein, wenn der interne Server umkonfiguriert werden musste.

Legen Sie anschließend das Netzwerk aus, von welchem die Anfragen kommen.



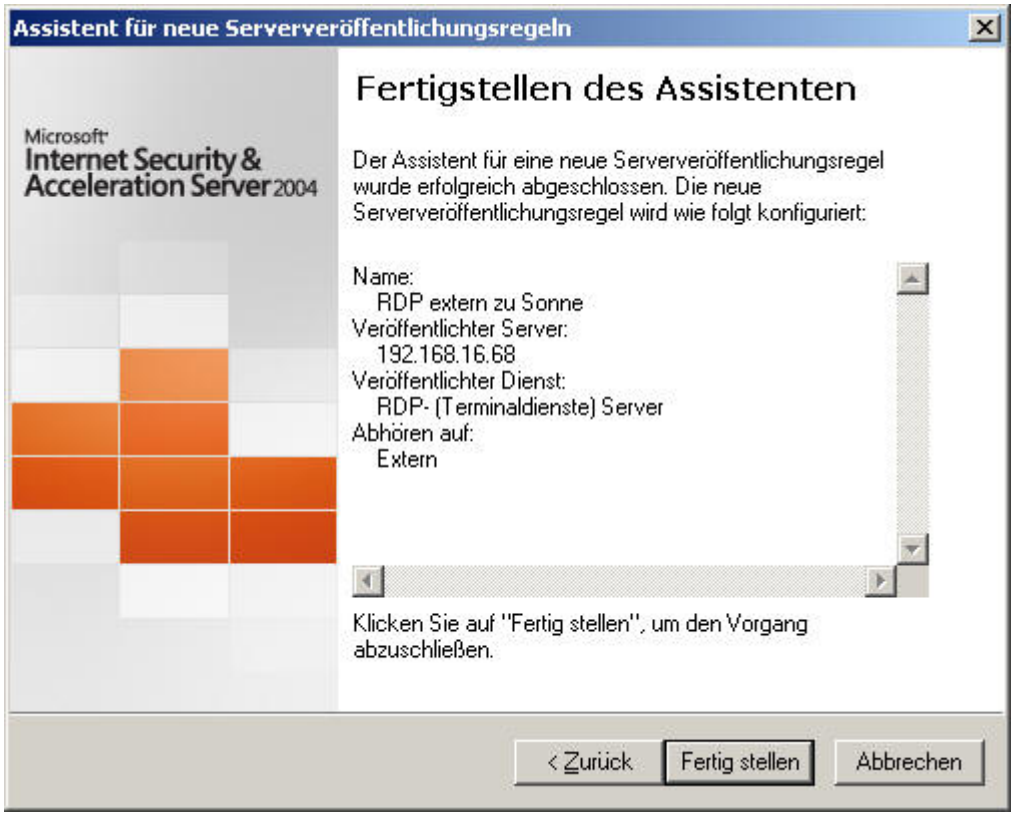
Hinweis: Sollte der ISA Server über mehrere externe IP-Adressen verfügen, können Sie mittels "Adresse..." festlegen, auf welcher IP-Adresse RDP-Anfragen entgegengenommen werden:



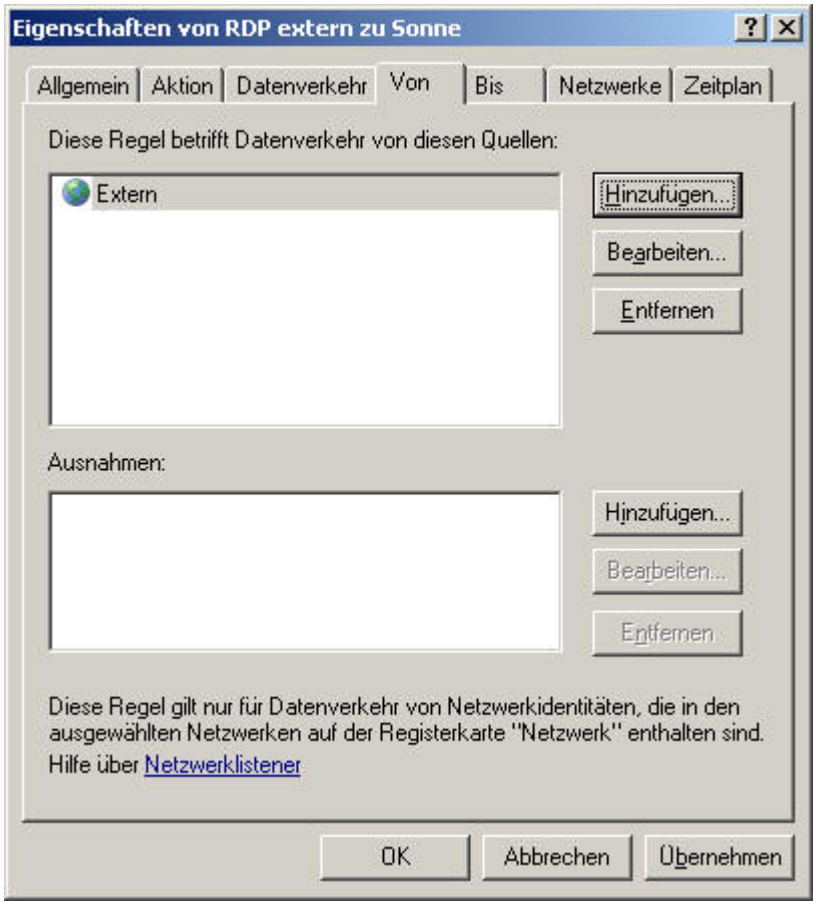


Hinweis: Sollten Sie mehrere interne Server (oder den ISA Server Computer) gleichzeitig per RDP von extern zugänglich machen, müssen Sie dafür unterschiedliche externe IP-Adressen oder einen anderen Port verwenden. Sie können mit einer externen IP Adresse maximal einen internen Server veröffentlichen.

Die letzte Seite des Assistenten zeigt wie immer eine Übersicht an.



Bevor die neu erstelle Firewallrichtlinie übernommen wird, sollten Sie noch eine kleine Korrektur in den Eigenschaften der Richtlinie vornehmen. Gehen Sie dazu auf die Registerkarte "Von".



Standardmäßig wird als Quellnetzwerk "beliebig" ausgewählt. Ändern Sie das in "Extern" ab. Sollten Sie noch weitere Einschränkungen vornehmen wollen, so tun Sie es hier und jetzt. Es ist z.B. denkbar, dass Sie nur bestimmte vordefinierte Computer in einem Computersatz zusammenfassen und nur diesen den Zugriff auf diese Regel erlauben. Dann würden Sie natürlich diesen Computersatz statt "Extern" hinzufügen.

Denken Sie daran, die durchgeführten Änderungen zu übernehmen. Erst dann wird das Regelwerk in ISA Server tatsächlich geändert und steht zur Verfügung.

Sollten Sie eine Fehlkonfiguration gefunden haben, können Sie alle getätigten aber noch nicht gespeicherten Änderungen wieder verwerfen.

Vom Client aus ruft man einfach die "Remotedesktopverbindung" (Start -> Programme -> Zubehör -> Kommunikation) auf (alternativ: `mstsc`) und gibt den Namen oder die IP-Adresse und mit einem Doppelpunkt getrennt den alternativen Port des ISA Servers ein:

Tip: Mit dem Befehl `mstsc /console` ruft man eine Remotedesktopverbindung auf die Konsole auf. Das hat mehrere Vorteile:

- *man sieht Popups/Warnungen*
- *man kann meist Software installieren, die nicht im Terminalmodus installiert werden kann*
- *man kann die Konsole so übernehmen/übergeben wie man sie am "echten" Monitor sieht*

Übersicht über die ISA Server 2004 Monitoring Funktionen

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

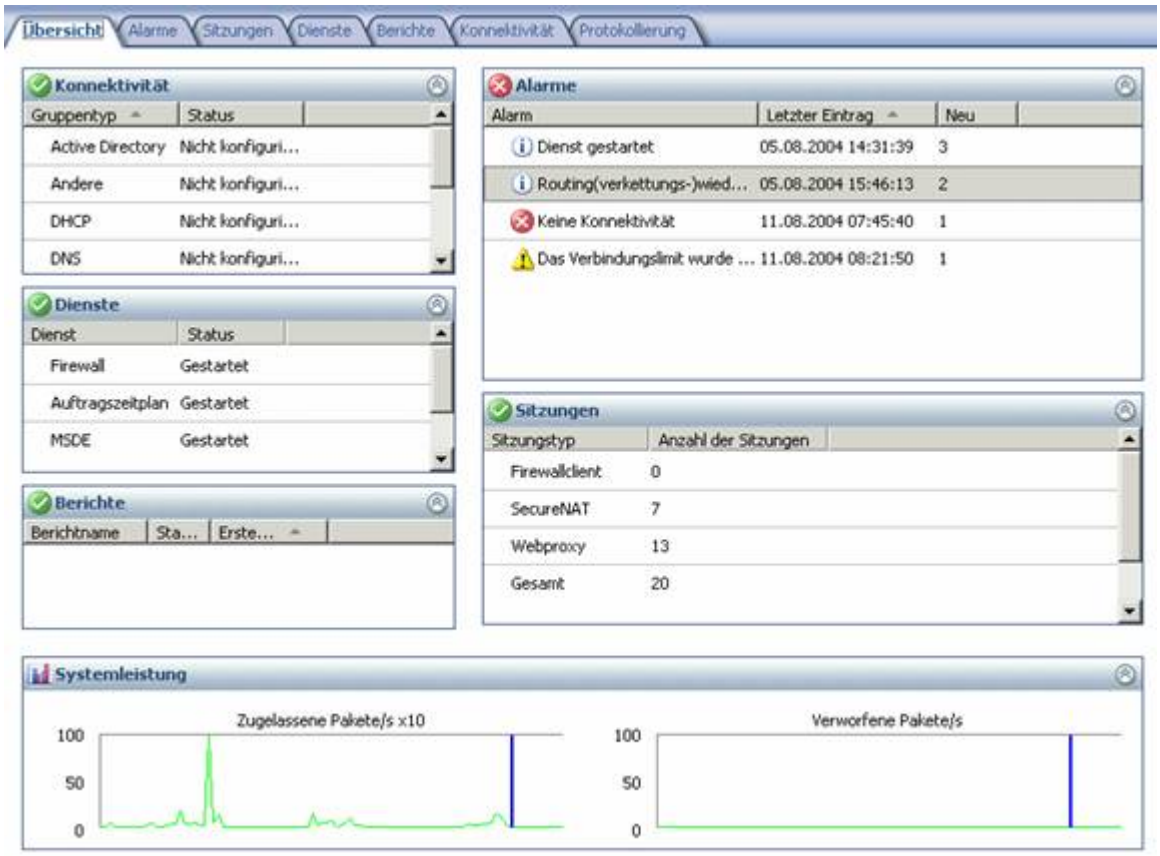
Der Microsoft ISA Server 2004 bietet sehr umfangreiche Monitoring Möglichkeiten, um den Status der Firewall und des Proxy-Servers zu überwachen.

Im Vergleich zum ISA Server 2000 stehen jetzt leistungsfähige Analysetools zur Verfügung. Eines der Highlights ist die Möglichkeit, die ISA Protokolldaten in Echtzeit zu analysieren und mit Filtern nach den gewünschten Daten zu filtern.

Dashboard / Übersicht

Zentrale Anlaufstelle ist das so genannte „Dashboard“. In der Übersichtsansicht der ISA Server-Verwaltung wird in Echtzeit eine Momentaufnahme der zusammengefassten ISA Server-Aktivität angezeigt. Mit den übersichtlich auf einer Seite angeordneten wichtigen Informationen können Probleme schnell erkannt und behoben werden.

Das Dashboard und alle folgenden Monitoring Möglichkeiten befinden sich im Container „Überwachung“ des ISA Verwaltungstool unterhalb des ISA Server Computerobjektes.



Ich beschreibe jetzt die Funktion der einzelnen Fenster des ISA Dashboards:

Konnektivität:

ISA 2004 bietet die Möglichkeit zur Überprüfung der Konnektivität von wichtigen Systemen innerhalb der Organisation wie DHCP Server, DNS Server und Active Directory, sowie z. B. der Prüfung der Verfügbarkeit einer Website durch das Ausführen eines HTTP GET Befehls. Mit diesem Feature kann ein Administrator schnell reagieren, wenn unternehmenskritische Komponenten nicht erreichbar sind, von denen der ISA Server zum Beispiel abhängig sein könnte.

Dienste:

Listet den Status der installierten ISA 2004 Dienste auf.

Berichte:

ISA 2004 bietet die Möglichkeit der Definition so genannter Berichtsaufträge mit welchen man sich zum Beispiel die protokollierte Internetaktivität in grafisch aufbereiteter Form anzeigen lassen kann. Dieses Feature ist sehr hilfreich zur Präsentation von Daten für Führungsstellen oder einfach nur zur Übersicht für den Firewall-Administrator. Das Dashboard zeigt den Status der konfigurierten Berichtsaufträge an.

Systemleistung:

Die Systemleistung zeigt zwei Zähler des Systemmonitors an.

- Zugelassene Pakete pro Sekunde x10 zeigt die Datenmengen an, welche der ISA pro Sekunde durch die Firewallengine führt.
- Verworfene Pakete pro Sekunde zeigen die Datenmengen an, welche der ISA pro Sekunde an der Firewall verweigert (verwirft).

Bemerkung:

Eine hohe Anzahl verworfener Pakete ist häufig ein Anzeichen für Denial of Service (DoS) Angriffe auf den ISA Server.

Alarme:

Hier werden ISA Server Systemmeldungen angezeigt, welche für den einwandfreien ISA Betrieb sehr wichtig sind. Wie man der Grafik entnehmen kann, werden hier z. B. gestartete ISA Dienste angezeigt oder Informationen über Webverkettungsprobleme uvm.

Sitzungen:

Hier wird die Anzahl der Verbindungen (Sitzungen) der drei ISA 2004 Clientarten

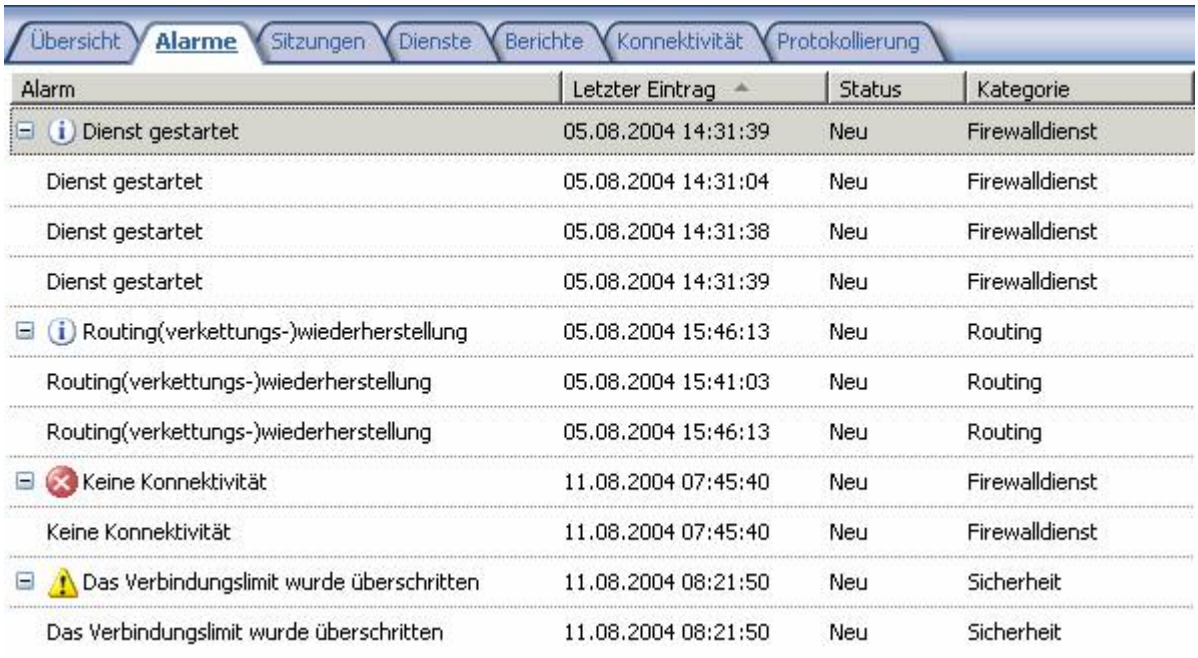
- SecureNAT Client
- Firewall Client
- Webproxy Client

angezeigt.

Die Anzahl spiegelt nicht unbedingt die tatsächliche Anzahl der Client Computer wieder, weil ein Client mehrere Clientarten gleichzeitig verwenden kann.

Alarme

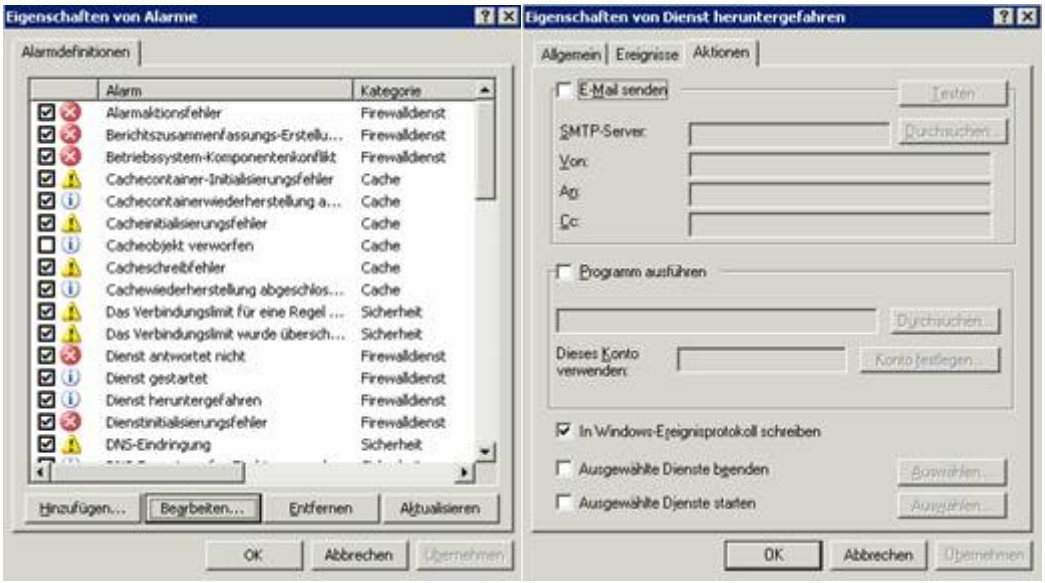
In der Registerkarte „Alarme“ protokolliert der ISA Server wichtige Systemereignisse wie das Starten und Beenden von ISA 2004 Diensten und zum Beispiel fehlende Konnectivität-Verbindungen. In der Spalte „Kategorie“ wird die beteiligte ISA 2004 Komponente angezeigt.



Alarm	Letzter Eintrag	Status	Kategorie
Dienst gestartet	05.08.2004 14:31:39	Neu	Firewalldienst
Dienst gestartet	05.08.2004 14:31:04	Neu	Firewalldienst
Dienst gestartet	05.08.2004 14:31:38	Neu	Firewalldienst
Dienst gestartet	05.08.2004 14:31:39	Neu	Firewalldienst
Routing(verkettungs-)wiederherstellung	05.08.2004 15:46:13	Neu	Routing
Routing(verkettungs-)wiederherstellung	05.08.2004 15:41:03	Neu	Routing
Routing(verkettungs-)wiederherstellung	05.08.2004 15:46:13	Neu	Routing
Keine Konnektivität	11.08.2004 07:45:40	Neu	Firewalldienst
Keine Konnektivität	11.08.2004 07:45:40	Neu	Firewalldienst
Das Verbindungslimit wurde überschritten	11.08.2004 08:21:50	Neu	Sicherheit
Das Verbindungslimit wurde überschritten	11.08.2004 08:21:50	Neu	Sicherheit

Der ISA 2004 bietet auch ausgefeilte Benachrichtigungsoptionen, welche bei Erreichen eines bestimmten Systemzustandes aktiv werden.

Etwas versteckt befindet sich in der Taskbar die Möglichkeit, Alarmdefinitionen zu konfigurieren. Mit Hilfe dieser Konfiguration kann sich der ISA Administrator bei dem Eintreten bestimmter Ereignisse z. B. per E-Mail informieren zu lassen.



Neben der Möglichkeit eine E-Mail Benachrichtigung kann bei Erreichen des konfigurierten Alarms auch ein Programm ausgeführt werden, Informationen in das Windows Ereignisprotokoll geschrieben und z. B. bestimmte Dienste beendet werden. Aus Sicherheitsgründen kann es empfehlenswert sein, bei einem Angriff auf den ISA Server welche die Funktionalität des Systems kompromittiert, die ISA Firewalldienste zu Beenden. Dann ist zwar keine Internetkonnektivität mehr möglich, der ISA und das dahinterliegende LAN vor Angriffen geschützt. Das Beenden der Firewalldienste sollte auf alle Fälle in der Security Policy der EDV Abteilung vermerkt werden und von der Geschäftsführung abgesegnet sein.

Der ISA Server 2004 macht von dem Beenden des Firewallengine Dienstes Gebrauch, wenn z. B. das Firewall Logging nicht mehr gewährleistet ist

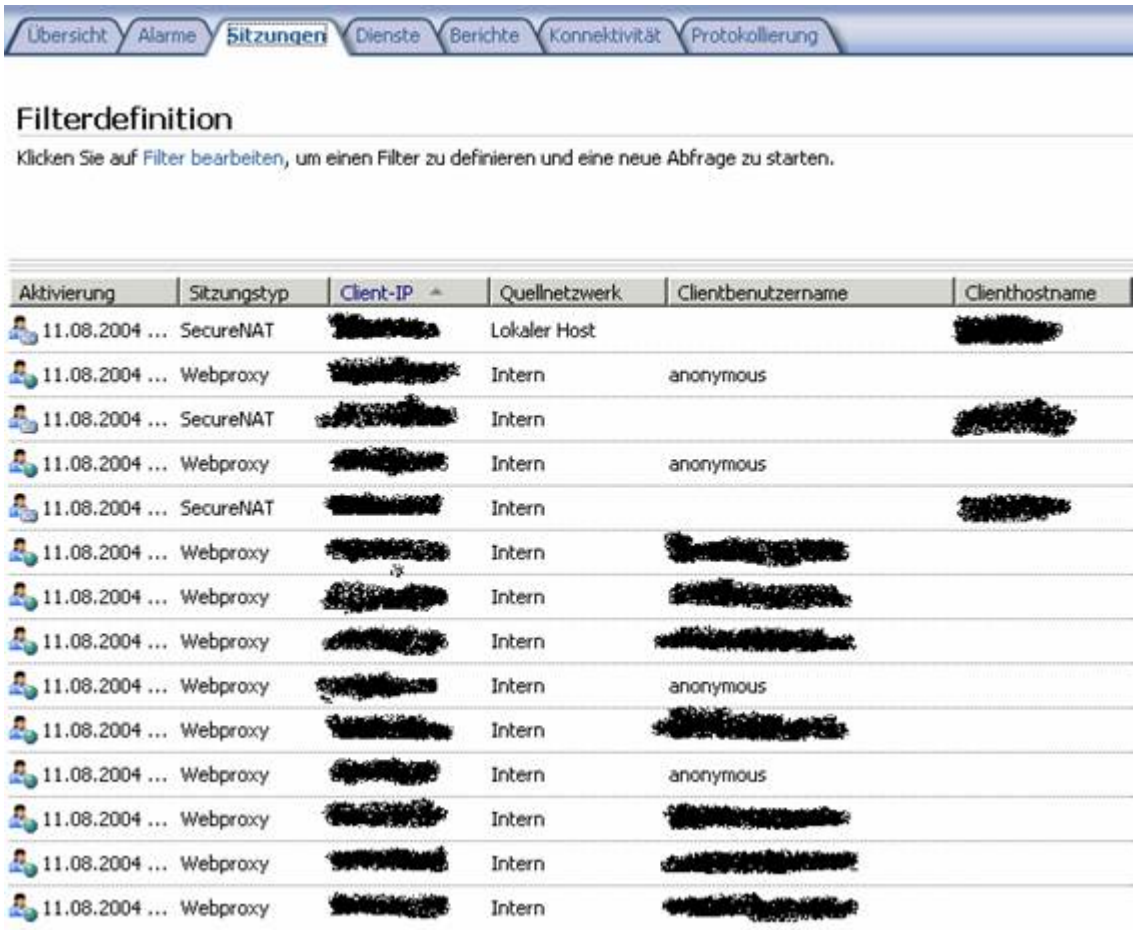
Sitzungen

Im Reiter „Sitzungen“ werden alle Verbindungen zum ISA Server 2004 angezeigt.

ISA 2004 zeigt hier den Verbindungszeitpunkt, den Sitzungstyp, die Client IP Adresse und viele weitere Informationen an.

Mit einem Rechtsklick auf eine der Spaltenüberschriften besteht die Möglichkeit, selbst Spalten hinzuzufügen bzw. zu entfernen. Es ist ebenfalls möglich die Spalten individuell zu verschieben.

Über den Punkt „Filter bearbeiten“ kann man eigene Abfragen definieren um das Suchergebnis zum Beispiel einzuschränken.



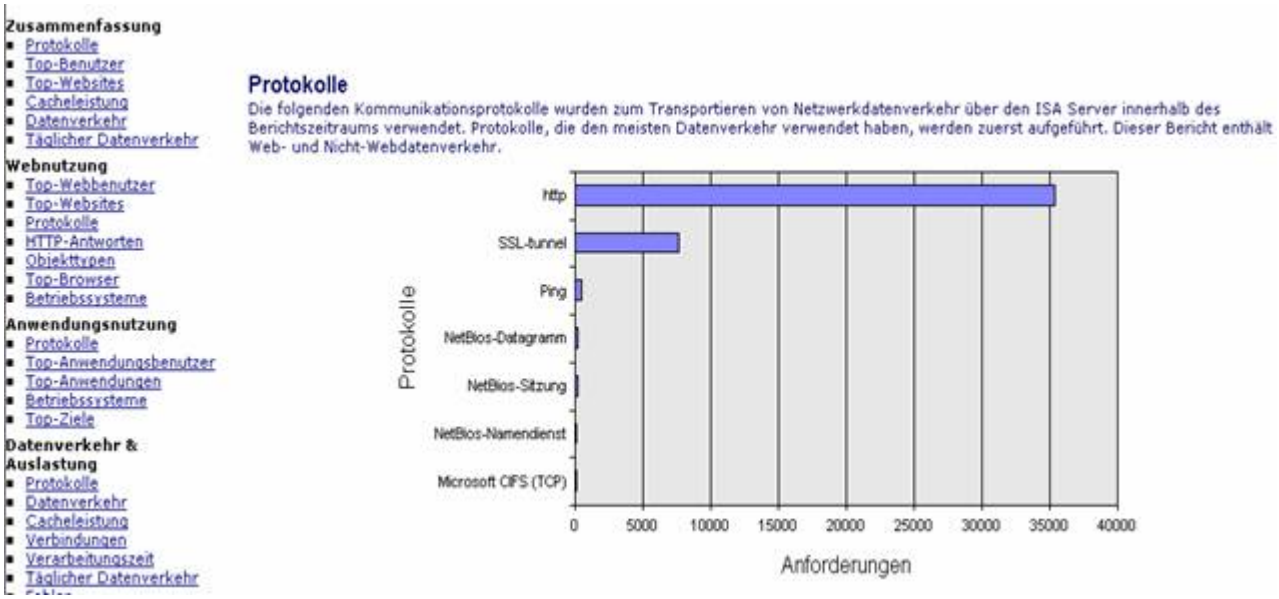
Dienste

In dem Reiter „Dienste“ kann man sich den Status der einzelnen ISA 2004 Dienste anzeigen lassen und jeden der Dienste Starten und Beenden.

Berichte

ISA 2004 bietet die Möglichkeit der Definition von so genannten Berichtsaufträgen mit dessen Hilfe man sehr einfach grafische HTML Reports generieren kann. Berichtsaufträge sind ein sehr nützliches Werkzeug um sich zum Beispiel die Top 10 der am meisten aufgesuchten Webseiten anzuzeigen oder den Prozentsatz der eingesetzten Webbrowser.

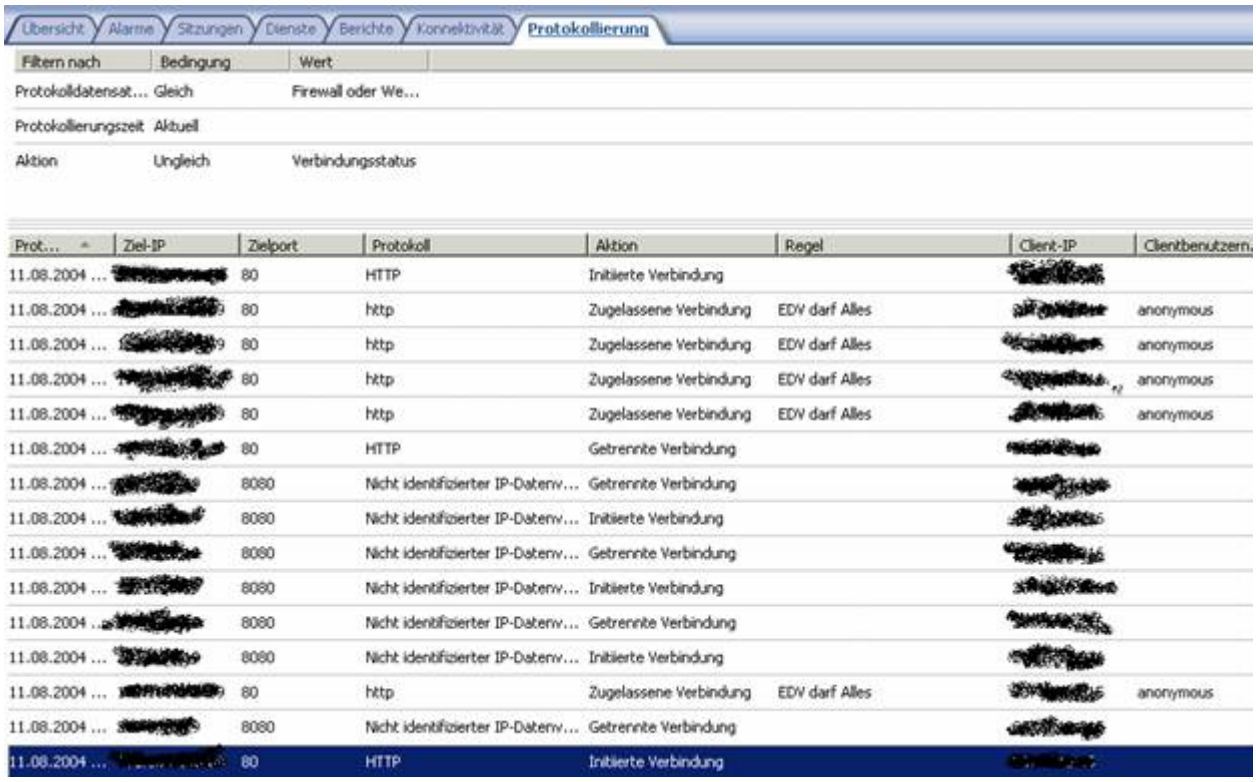
Durch einen Doppelkick auf den Berichtsnamen „Gesamtstatus“ öffnet sich nach kurzer Zeit der Webbrowser mit einem detailliertem HTML Report.



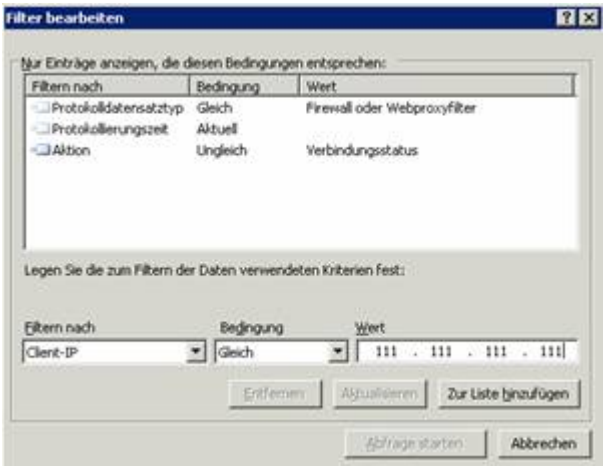
Protokollierung

Der Reiter „Protokollierung“ zeigt den Datenverkehr von und zum ISA 2004 endlich in „Echtzeit“ an. Über sehr umfangreiche Filter besteht die Möglichkeit, die angezeigten Protokolldaten zu modifizieren.

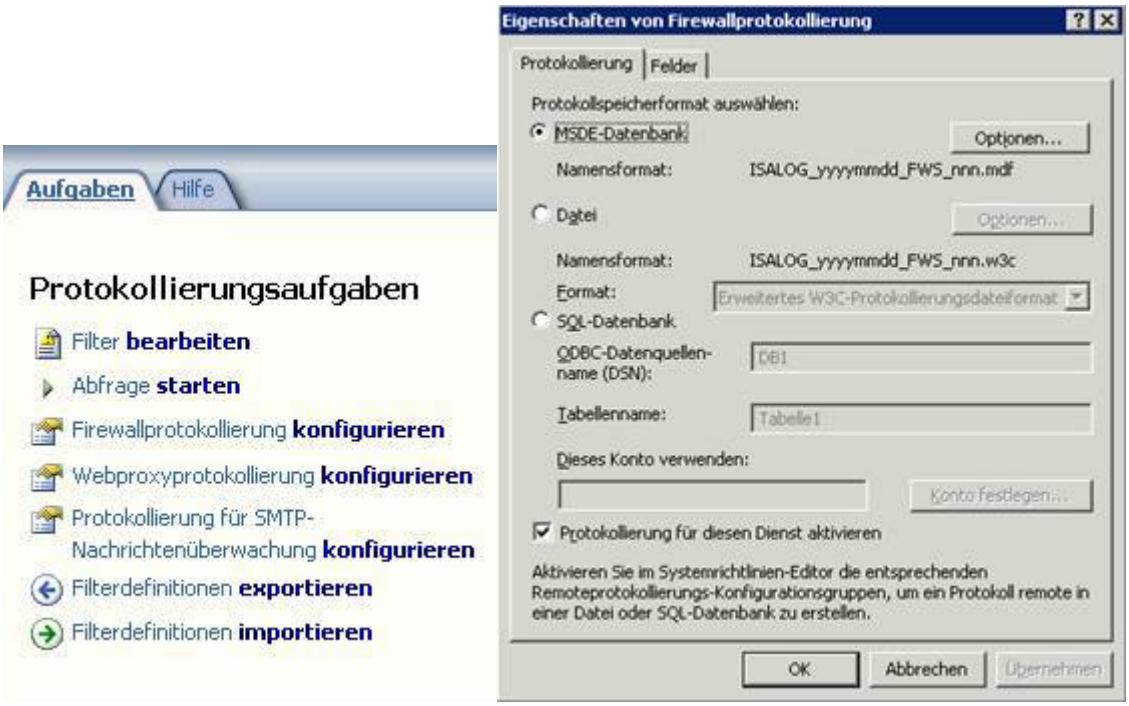
Auch hier besteht wieder die Möglichkeit durch einen Rechtsklick auf eine Spaltenüberschrift, Spalten hinzuzufügen und zu entfernen.



Über die sehr umfangreichen Filtermöglichkeiten kann man die Anzeige der geloggten Daten modifizieren um eine effektivere Suche zu ermöglichen.



Es besteht die Möglichkeit, die Art des Loggings am ISA Server 2004 zu modifizieren. Per Default protokolliert der ISA 2004 die Protokolldaten in eine per Default installierte MSDE Version.



Was wird protokolliert

Der Administrator kann an verschiedenen Stellen des Systems festlegen, welche Informationen protokolliert werden soll.

Generell besteht für jede Firewall Regel die Möglichkeit, auf dieser Regel basierenden Datenverkehr zu protokollieren. Per Default ist auch jede Regel „Protokoll aktiviert“.

Per Default werden auch die ISA 2004 eigenen Systemrichtlinienregeln protokolliert. Um die Systemrichtlinienregeln anzeigen zu lassen muss man im ISA Verwaltungstool unterhalb des ISA Computerobjektes mit der rechten Maustaste auf „Firewallregel“ klicken und im Kontextmenü – Ansicht – Systemrichtlinien Regeln anzeigen – aktivieren. Danach kann für die gewünschte Regel im Reiter „Aktion“ die Protokollierung deaktiviert werden.

Zu guter Letzt ist es auch noch möglich, verworfene Pakete zu protokollieren. ISA 2004 protokolliert per Default jedes verworfene Paket.

Die Einstellung, ob verworfene Pakete protokolliert werden sollen, wird ebenfalls im ISA Verwaltungstool eingestellt. Der Weg zur Konfiguration lautet:

ISA Computer Objekt – Konfiguration – Allgemein – „Erkennung von Eindringversuchen und DNS Angriffen aktivieren“. Dort kann man im Reiter „Allgemeine Angriffe“ „Verworfene Pakete protokollieren“.

Bemerkung:

Es ist immer wichtig, das „gesunde Maß“ an dem Verhältnis zwischen protokollierten Daten und dem Verzicht auf Protokollierung zu finden. Zuviel Protokollierung führt zu unübersichtlichen Logdateien, verlangsamt das System und führt schnell zu überschriebenen Logdateien wenn das GrößenLimit der Protokolldatei erreicht ist.

Die Default Logdateigröße für das Firewall- und Webproxy Log beträgt 8 GB. Beide Logs werden in einer MSDE protokolliert. Nur die Logdatei für die SMTP Nachrichtenüberwachung wird im erweiterten W3C Format geschrieben.

Konfiguration einer Konnektivitätsverifizierung

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Im Artikel Übersicht Monitoring wurde eine Zusammenfassung aller Überwachungsfunktionen des ISA Server 2004 gegeben. Das vorliegende Kapitel beschreibt die Möglichkeit, den ISA so einzurichten, dass er bestimmte andere Server oder Dienste auf deren Verfügbarkeit überprüft und je nach Zustand Maßnahmen ergreift.

Es gibt drei Methoden zur Überprüfung der Konnektivität:

- HTTP-"GET"-Anforderung senden.
  Wenn diese Methode konfiguriert wurde, sendet ISA Server eine HTTP-GET-Anforderung und wartet auf die Antwort. Mit dieser Methode können Sie überprüfen, ob ein Webserver ausgeführt wird und für ISA Server erreichbar ist.

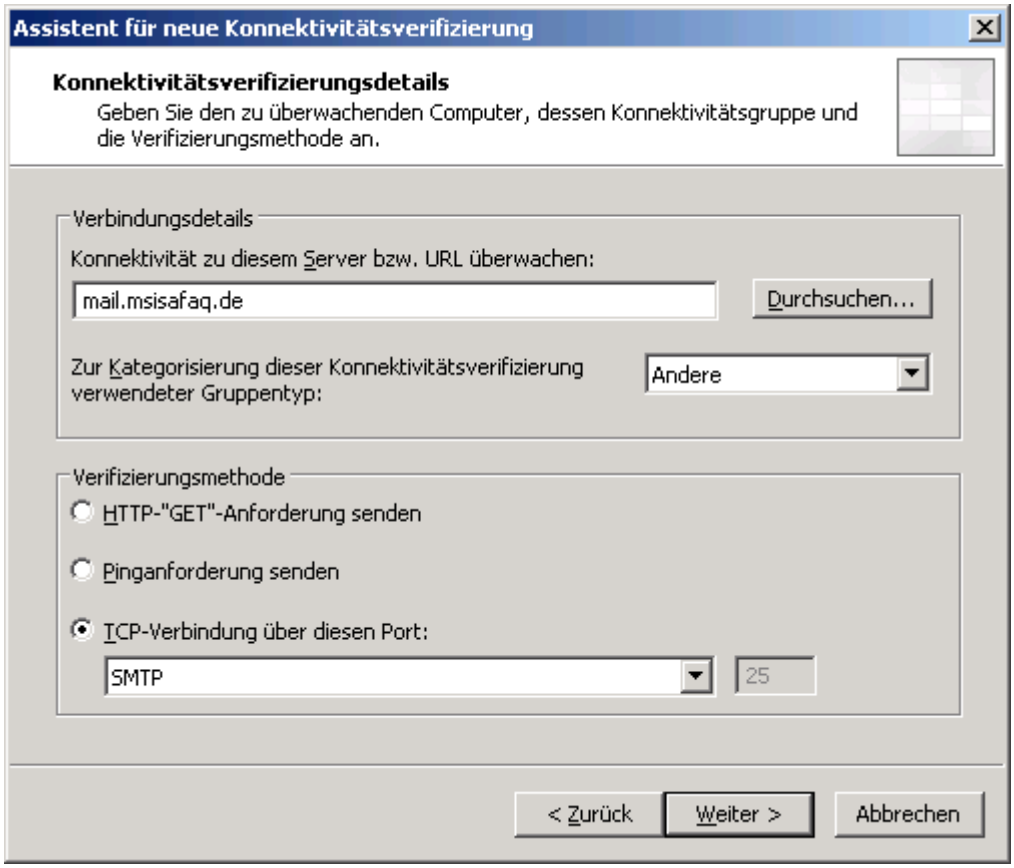
- Pinganforderung senden.
  Wenn diese Methode konfiguriert wurde, sendet ISA Server eine Anforderung (ICMP ECHO_REQUEST) an den angegebenen Server und wartet auf die entsprechende Antwort (ICMP ECHO_REPLY). Mit dieser Methode können Sie überprüfen, ob ein Server ausgeführt wird und für ISA Server erreichbar ist.

- TCP-Verbindung über dieses Protokoll herstellen.
  Wenn diese Methode konfiguriert wurde, versucht ISA Server, eine TCP-Verbindung mit einem bestimmten Port auf dem angegebenen Server herzustellen. Mit dieser Methode können Sie überprüfen, ob ein bestimmter Dienst auf dem Server ausgeführt wird und für ISA Server erreichbar ist.

Um eine neue Konnektivitätsverifizierung einzurichten oder sich bestehende anzeigen zulassen, wählt man die Registerkarte "Konnektivität" im Knoten "Überwachung" der ISA Server Management Konsole aus.

In diesem Beispiel ist noch keine Überprüfung konfiguriert. Somit kann nur entweder eine neue erstellt werden oder es kann eine (z.B. von einem anderen ISA Server exportierte) XML-Datei mit Überprüfungsregeln importiert werden.

Die erste Seite des Assistenten verlangt wie immer die Eingabe eines Regelnamens. Hier sollte (wie immer) ein "sprechender" Name eingetragen werden.

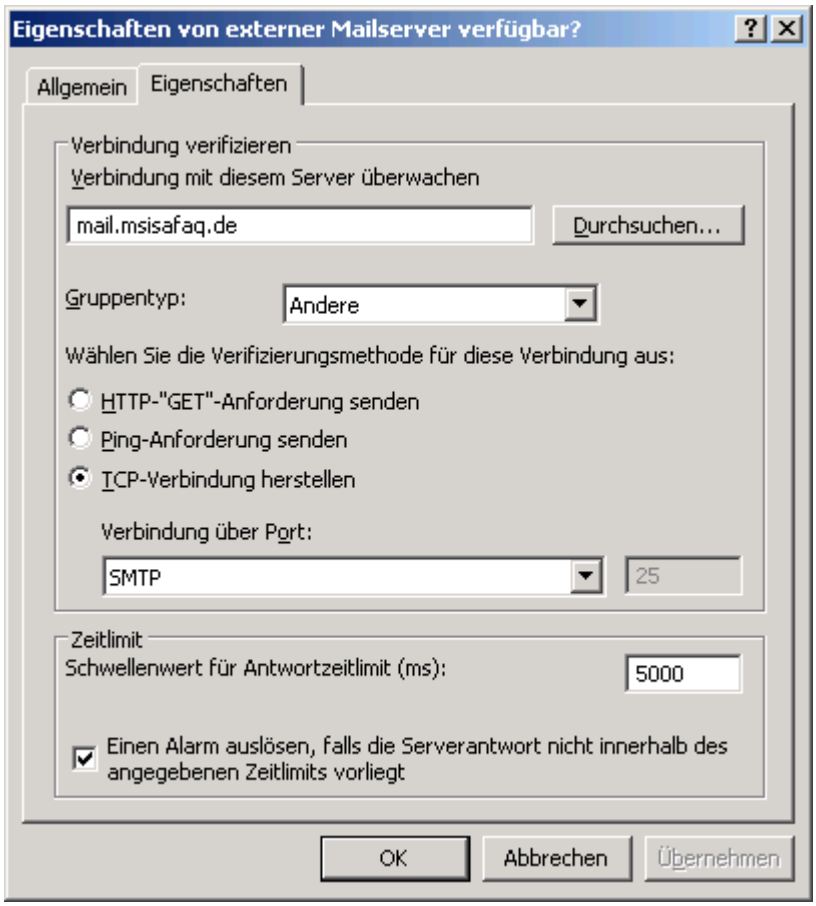


In den Verbindungsdetails kann man entweder einen FQDN oder eine IP Adresse des zu überwachenden Systems angeben. Ebenso kann mittels der "Durchsuchen"-Funktion ein Ziel im AD ausgewählt werden. Im oberen Beispiel soll die Verfügbarkeit des externen Mailservers überprüft werden.

Beim Konfigurieren einer Konnektivitätsverifizierung für einen Server kann diese in eine der folgenden Gruppen eingestuft werden: Active Directory, DHCP, DNS, Veröffentlichte Server, Web (Internet) und Andere. Der Servergruppenstatus wird in der Übersichtsansicht (Dashboard) angezeigt.

Zum Schluss die übliche Zusammenfassungsmeldung mit allen eingegebenen Details.

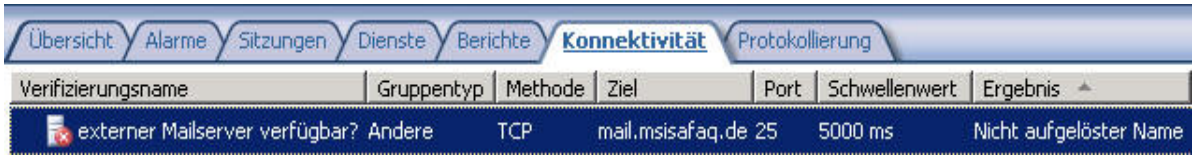
Lässt man sich anschließend die Eigenschaften der neu erstellten Regel anzeigen, kann man noch zwei weitere Optionen konfigurieren:



Zum einen kann der Schwellenwert konfiguriert werden, nach dem der ISA Server de Verbindung als nicht zustande gekommen ansieht. Ergänzend dazu kann noch festgelegt werden, ob bei einem Fehler ein Alarm ausgelöst wird. Wenn nicht, wird lediglich in der Management Konsole eine Warnung ausgegeben.

Damit die Überprüfungsregel aktiv wird, muss - wie immer bei einer Konfigurationsänderung - diese übernommen werden:

Anschließend wird die Regel ausgeführt.



In diesem Beispiel wurde festgestellt, dass der zu überprüfende Mailserver nicht erreichbar ist. Als Grund (-> Ergebnis) wird genannt: "Nicht aufgelöster Name". Folgende Ergebnisse können gemeldet werden:

- Verifizierung
  In diesem Moment wird die Regel angewendet und der Zielserver überprüft
- x ms
  x gibt die Zeitspanne in Millisekunden an, innerhalb der eine Antwort empfangen wurde
- Fehler
  Der Zielserver konnte nicht erreicht werden (Deutet meist auf ein temporäres Problem oder eine erforderliche Proxyauthentifikation hin)

Folgende Tabelle (aus der Online Hilfe) gibt Auskunft, welches Ergebnis bei einer HTTP-Anfrage in Abhängigkeit der Rückmeldung des Webservers geliefert wird:

HTTP-Antwort vom überwachten Server	**Konnektivitätsverifizierungsstatus**
1xx, 2xx oder 3xx	OK. Dies ist die Antwortzeit in Millisekunden.
401 (Webserverauthentifizierung erforderlich)	OK. Dies wird nicht als Fehler eingestuft, da die Meldung vom Webserver zurückgegeben wurde.
407 (Proxyauthentifizierung erforderlich)	Fehler (Windows Server 2003). Dies wird als Fehler eingestuft, da die Konnektivität zum eigentlichen Webserver nicht ermittelt werden kann.
407 (Proxyauthentifizierung erforderlich)	Authentifizierung erforderlich (Windows 2000 Server).
4xx (außer 401 und 407) oder 5xx	Fehler
Zeitüberschreitung der Anforderung	Zeitüberschreitung
Der Servername konnte nicht aufgelöst werden	Nicht aufgelöster Name.
ISA Server ist nicht verfügbar	Verifizierung nicht möglich (Firewalldienst ist nicht verfügbar)

Sofern die Alarmfunktion nicht deaktiviert wurde, wird bei einem Verbindungsfehler ein Alarm angezeigt:

Abhängig von diesem Alarmevent können dann verschiedene Maßnahmen eingeleitet werden. Damit wird sich ein eigenständiger Artikel beschäftigen.

Unabhängig von der Alarmierung wird der Status der Konnektivitätsverifizierung im Dashboard angezeigt:

Konnektivität
Gruppentyp
Status
Active Directory
Gut
Andere
Keine Verbindung
DHCP
Gut
DNS
Gut
Veröffentlichte Server
Nicht konfiguriert
Web (Internet)
Nicht konfiguriert

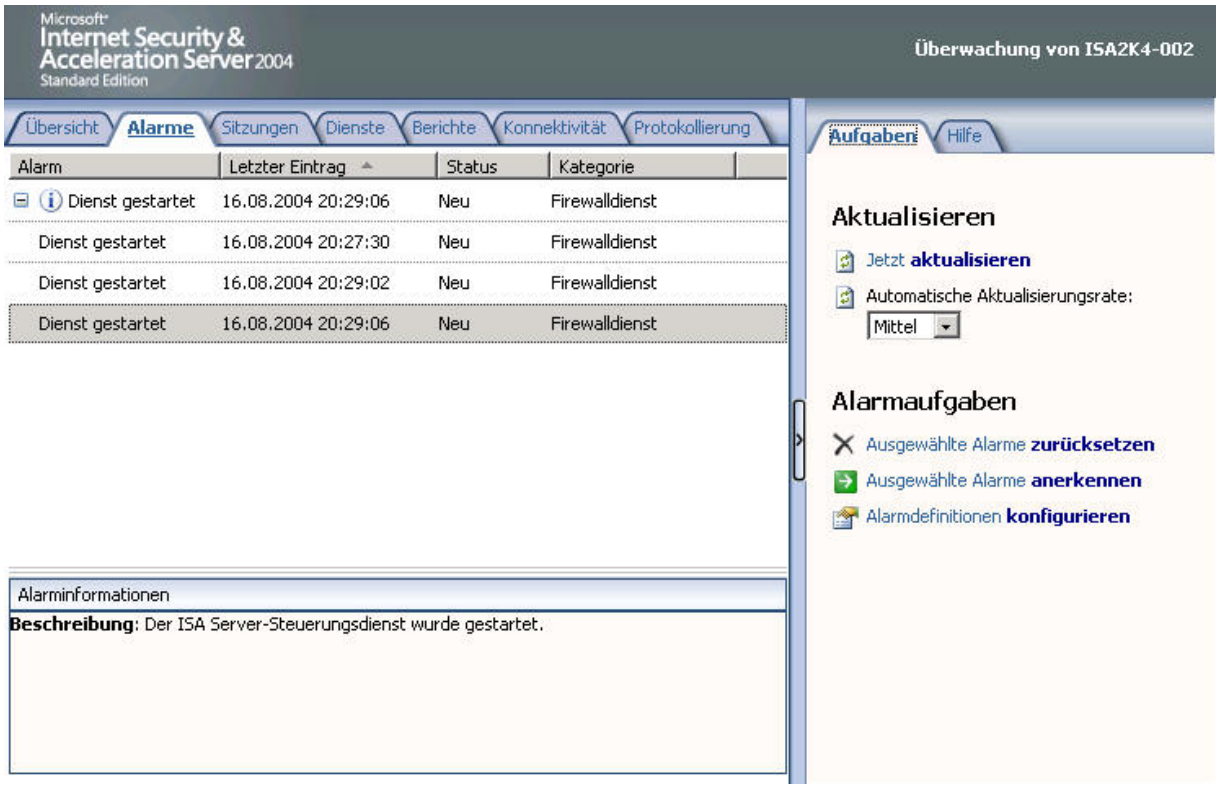
Alarmkonfiguration

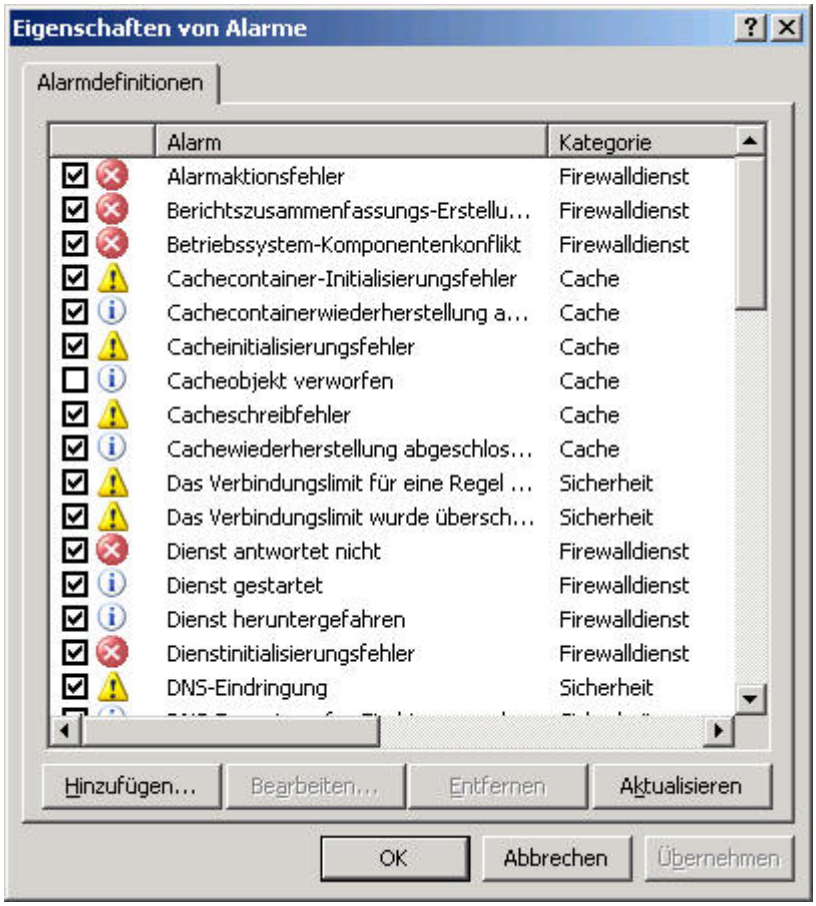
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Der ISA Server bietet die Möglichkeit, eine vordefinierte Reaktion auf ein bestimmtes Ereignis auszuführen. Der ISA Server-Alarmdienst fungiert dann als Verteiler und als Ereignisfilter. Er ist für das Erfassen von Ereignissen verantwortlich, überprüft die Erfüllung bestimmter Bedingungen (z.B. Schwellenwerte) und führt die entsprechenden Aktionen aus. Eine solche Aktion kann zum Beispiel ein Eintrag im Ereignisprotokoll oder eine E-Mail an den Firewalladministrator sein.

Um dem Administrator etwas Arbeit abzunehmen, liefert der ISA Server serienmäßig eine ganze Reihe Alarmdefinitionen mit. Um die Alarmdefinitionen zu konfigurieren öffnen Sie den Aufgabenbereich im Knoten Überwachung -> Alarme:

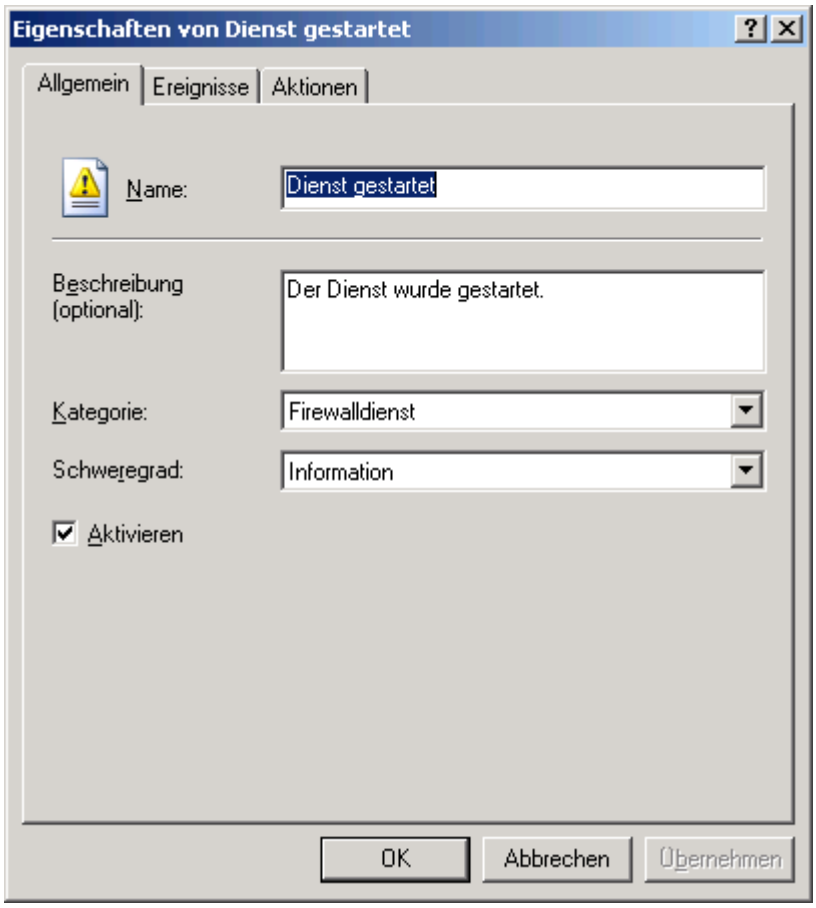




Hier eine Aufstellung der im Auslieferungszustand enthaltenen Alarmdefinitionen und deren Aktivierungsstatus:

Alarmaktionsfehler	Firewalldienst
Berichtszusammenfassungs-Erstellu…	Firewalldienst
Betriebssystem-Komponentenkonflikt	Firewalldienst
Cachecontainer-Initialisierungsfehler	Cache
Cachecontainerwiederherstellung a…	Cache
Cacheinitialisierungsfehler	Cache
Cacheobjekt verworfen	Cache
Cacheschreibfehler	Cache
Cachewiederherstellung abgeschlos…	Cache
Das Verbindungslimit für eine Regel …	Sicherheit
Das Verbindungslimit wurde übersch…	Sicherheit
Dienst antwortet nicht	Firewalldienst
Dienst gestartet	Firewalldienst
Dienst heruntergefahren	Firewalldienst
Dienstinitialisierungsfehler	Firewalldienst
DNS-Eindringung	Sicherheit
DNS-Zonentransfer-Eindringversuch	Sicherheit
Ein Neustart des ISA Server-Compu…	Firewalldienst
Eindringversuch festgestellt	Sicherheit
Ereignisprotokollfehler	Firewalldienst
Ermittlungsmechanismus gegen bös…	Sicherheit
Fehler bei der Cachedatei-Größenä…	Cache
Fehler bei Wählen bei Bedarf	Firewalldienst
Firewallkommunikationsfehler	Firewalldienst
FTP-Filter-Initialisierungswarnung	Firewalldienst
IP-Spoofing	Sicherheit
Keine Konnektivität	Firewalldienst
Keine Ports verfügbar	Firewalldienst
Komponentenladefehler	Firewalldienst
Konfigurationsfehler	Firewalldienst
Langsame Konnektivität	Firewalldienst
Nicht registriertes Ereignis	Firewalldienst
POP-Eindringversuch	Sicherheit
Protokollierungsfehler	Firewalldienst
Protokollspeicherlimits	Firewalldienst
Ressourcenzuweisungsfehler	Firewalldienst
Routing(verkettungs-)fehler	Routing
Routing(verkettungs-)wiederherstel…	Routing
RPC-Filter - Bindungsfehler	Firewalldienst
RPC-Filter: Konnektivität wurde geä…	Firewalldienst
Serververöffentlichung ist unzutref…	Firewalldienst
Serververöffentlichung-Wiederhers…	Firewalldienst
Serververöffentlichungsfehler	Firewalldienst
SMTP-Filterereignis	Firewalldienst
SOCKS-Konfigurationsfehler	Firewalldienst
SYN-Angriff	Sicherheit
Ungültige Anmeldeinformationen für…	Firewalldienst
Ungültige ODBC-Protokoll-Anmeldei…	Firewalldienst
Ungültige Zertifikatliste gefunden	Firewalldienst
Ungültiges DHCP-Angebot	Sicherheit
Upstreamverkettungs-Anmeldeinfor…	Firewalldienst
Veränderte Netzwerkkonfiguration	Firewalldienst
VPN-Verbindungsfehler	Firewalldienst
Zu großes UDP-Paket	Sicherheit
Änderungen des Quarantänen-VPN…	Firewalldienst

Bevor wir eine neue Alarmdefinition hinzufügen sollten wir uns die bestehenden am Beispiel von "Dienst gestartet" einmal genauer ansehen:



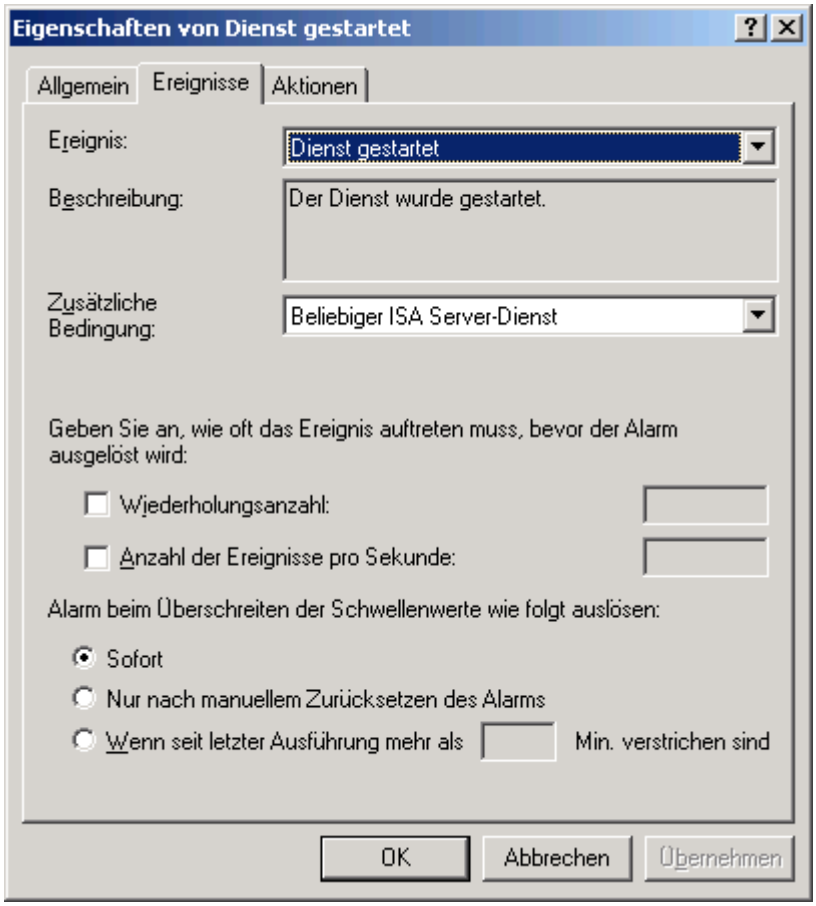
Auf der ersten Registerkarte werden Name, Beschreibung, Kategorie sowie die Information über den Schweregrad des Alarms angegeben. Hier kann außerdem der Alarm aktiviert oder deaktiviert werden, was auch in der Übersicht durch setzen oder löschen des Häkchens getätigt werden kann.

Folgende Kategorien stehen zur Auswahl:

- Sicherheit
- Cache
- Routing
- Firewalldienst
- Andere

Folgende Schweregrade stehen zur Verfügung:

- Fehler
- Warnung
- Information



Auf der zweiten Registerkarte wird der Alarm näher spezifiziert und ein Ereignis wird zugrunde gelegt.

Folgende Ereignisse sind wählbar (Auszug aus der Online-Hilfe):

Ereignis	**Beschreibung**
Alarmaktionsfehler	Die dem Alarm zugeordnete Aktion ist fehlgeschlagen.
Cachecontainer-Initialisierungsfehler	Die Cachecontainerinitialisierung ist fehlgeschlagen und die Initialisierung wurde ignoriert.
Cachecontainerwiederherstellung abgeschlossen	Die Wiederherstellung eines einzelnen Cachecontainers wurde abgeschlossen.
Fehler bei der Cachedatei-Größenänderung	Die Größe der Cachedatei konnte nicht verkleinert werden.
Cacheinitialisierungsfehler	Der Webcacheproxy wurde aufgrund eines globalen Fehlers deaktiviert.
Cachewiederherstellung abgeschlossen	Der Cacheinhalt wurde wiederhergestellt.
Cacheschreibfehler	Der Versuch, Inhalt in den Cache zu schreiben, ist fehlgeschlagen.
Cacheobjekt verworfen	Während der Cachewiederherstellung wurde ein Objekt mit in Konflikt stehenden Informationen gefunden. Dieses Objekt wurde verworfen.
Komponentenladefehler	Eine Erweiterungskomponente konnte nicht geladen werden.
Konfigurationsfehler	Beim Lesen der Konfigurationsinformationen ist ein Fehler aufgetreten.
Das Verbindungslimit wurde überschritten	Ein Benutzer oder eine IP-Adresse hat das Verbindungslimit überschritten.

Das Verbindungslimit für eine Regel wurde überschritten	Die Anzahl der pro Sekunde für eine Regel zugelassenen Verbindungen wurde überschritten.
Ermittlungsmechanismus gegen bösartige DHCP-Eindringversuche wurde deaktiviert	Der Ermittlungsmechanismus gegen bösartige DHCP-Eindringversuche wurde deaktiviert.
Fehler bei Wählen bei Bedarf	Die DFÜ-Verbindung konnte nicht erstellt werden, da entweder keine Antwort empfangen wurde oder die Leitung besetzt ist.
DNS-Zonentransfer-Eindringversuch	Ein Zonentransferangriff ist aufgetreten.
Ereignisprotokollfehler	Die Ereignisinformationen konnten nicht im Systemereignisprotokoll protokolliert werden. In der Standardeinstellung ist dieser Alarm deaktiviert.
Firewallkommunikationsfehler	Zwischen dem Firewallclient und dem ISA Server-Dienst ist ein Kommunikationsfehler aufgetreten.
FTP-Filter-Initialisierungswarnung	Der FTP-Filter konnte die zugelassenen FTP-Befehle nicht analysieren. Vergewissern Sie sich, dass die Befehle im richtigen Format gespeichert sind. Befehle dürfen nicht mehr als 4 Zeichen lang sein und müssen durch ein Leerzeichen getrennt werden.
Eindringversuch festgestellt	Ein externer Benutzer hat versucht einzudringen.
Ungültige Zertifikatliste gefunden	Das Clientzertifikat wurde aufgrund einer ungültigen oder fehlenden Zertifikatsperrliste widerrufen. Möglicherweise ist die Zertifikatsperrliste abgelaufen, und es konnte keine gültige Zertifikatsperrliste gedownloadet werden. Stellen Sie sicher, dass die Konfigurationsgruppe für die Systemrichtlinie zum Downloaden von Zertifikatsperrlisten aktiviert ist und dass eine Verbindung zu den Sperrlisten-Verteilungspunkten besteht.
Ungültiges DHCP-Angebot	Die IP-Adresse des DHCP-Angebots ist ungültig.
Die Anmeldeinformationen für Wählen bei Bedarf sind ungültig.	Ungültige Anmeldeinformationen für Wählen bei Bedarf wurden ermittelt.
Ungültige ODBC-Protokoll-Anmeldeinformationen	Der angegebene Benutzername oder das Kennwort ist für diese ODBC-Datenbank ungültig.
IP-Spoofing	Die IP-Paketquelladresse ist ungültig.
Ein Neustart des ISA Server-Computers ist erforderlich.	Änderungen an der Konfiguration werden erst nach dem Neustart des Computers wirksam.
Protokollierungsfehler	Die Protokollierung für Dienstname ist fehlgeschlagen.
Protokollspeicherlimits	Mindestens ein Protokollspeicherlimit wurde erreicht.
Veränderte Netzwerkkonfiguration	Es wurde eine Netzwerkkonfigurationsänderung festgestellt, die ISA Server betrifft.
Keine Ports verfügbar	Es konnte kein Netzwerksocket erstellt werden, weil keine Ports verfügbar sind.
Keine Konnektivität	ISA Server konnte keine Verbindung mit dem angeforderten Server herstellen.
Betriebssystem-Komponentenkonflikt	Eine der folgenden Komponenten steht in Konflikt mit dem Betriebssystem: IP-Netzwerkadressübersetzung-Editor (NAT), Gemeinsame Nutzung der Internetverbindung (ICS) oder Routing und RAS (RRAS).
Zu großes UDP-Paket	Ein UDP-Paket (User Datagram Protocol) wurde von ISA Server verworfen, da es größer als die im Registrierungsschlüssel maximal zugelassene UDP-Paketgröße ist.
POP-Eindringversuch	Es wurde ein POP-Pufferüberlauf (Post Office Protocol) festgestellt.
Änderungen des Quarantänen-VPN-Clientnetzwerks	Ein Benutzer wurde aus dem Quarantänen-VPN-Clientnetzwerk entfernt. In der Standardeinstellung ist dieser Alarm deaktiviert.

Berichtszusammenfassungs-Erstellungsfehler	Beim Erstellen der Berichtzusammenfassung aus den Protokollierungsdateien ist ein Fehler aufgetreten.
Ressourcenzuweisungsfehler	Ein Ressourcenzuweisungsfehler ist aufgetreten. Möglicherweise stand nicht genügend Arbeitsspeicher zur Verfügung.
Routing(verkettungs-)fehler	ISA Server konnte die Anforderung nicht an einen Upstreamserver weiterleiten.
Routing(verkettungs-)wiederherstellung	ISA Server hat die Weiterleitung an einen Upstreamserver wieder aufgenommen.
RPC-Filter - Bindungsfehler	RPC-Filter kann den definierten Port nicht verwenden, da er bereits verwendet wird.
RPC-Filter: Konnektivität wurde geändert	Die Konnektivität zum Veröffentlichungs-RPC-Dienst Servername wurde geändert. Zusätzliche Schlüssel
Serververöffentlichungsfehler	Die Serververöffentlichungsregel wurde falsch konfiguriert.
Serververöffentlichung ist unzutreffend	Die Serververöffentlichungsregel kann nicht angewendet werden.
Serververöffentlichung-Wiederherstellung	Die Serververöffentlichungsregel kann jetzt angewendet werden.
Dienstinitialisierungfehler	Der Dienst konnte nicht initialisiert werden.
Dienst antwortet nicht	Ein ISA Server-Dienst wurde beendet bzw. unerwarteterweise angehalten.
Dienst heruntergefahren	Ein Dienst wurde ordnungsgemäß beendet. %Dienstname%
Dienst gestartet	Ein Dienst wurde ordnungsgemäß gestartet. %Dienstname%
Langsame Konnektivität	ISA Server hat eine langsame Verbindung mit dem angeforderten Server festgestellt.
SMTP-Filterereignis	Eine SMTP-Befehlsregel (Simple Mail Transfer Protocol) wurde verletzt.
SOCKS-Konfigurationsfehler	Der in den SOCKS-Eigenschaften angegebene Port wird von einem anderen Protokoll verwendet.
SYN-Angriff	Durch ISA Server wurde ein SYN-Angriff festgestellt.
Nicht registriertes Ereignis	Ein nicht registriertes Ereignis ist aufgetreten.
Upstreamverkettungs-Anmeldeinformationen	Die Upstreamverkettungs-Anmeldeinformationen sind ungültig.
VPN-Verbindungsfehler	Ein VPN-Clientverbindungsversuch ist fehlgeschlagen.

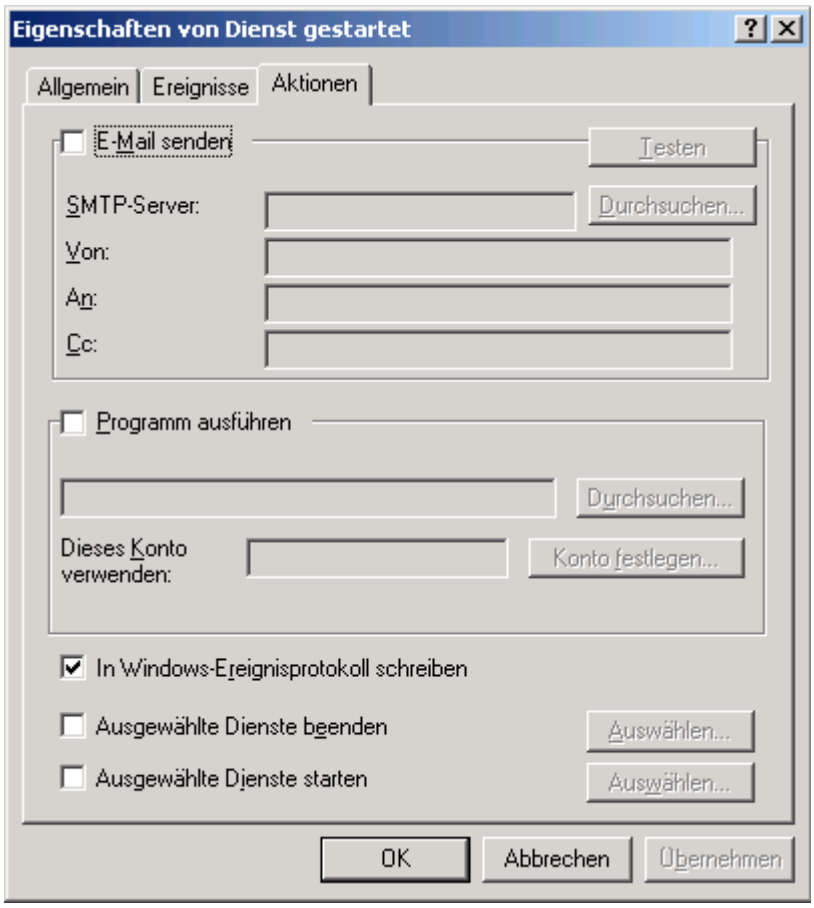
In Abhängigkeit des gewählten Ereignisses stehen verschiedene Auswahlmöglichkeiten als "Zusätzliche Bedingung" zur Verfügung.

Im Beispiel der Alarmdefinition für "Dienst gestartet" stehen folgende Bedingungen zur Verfügung:

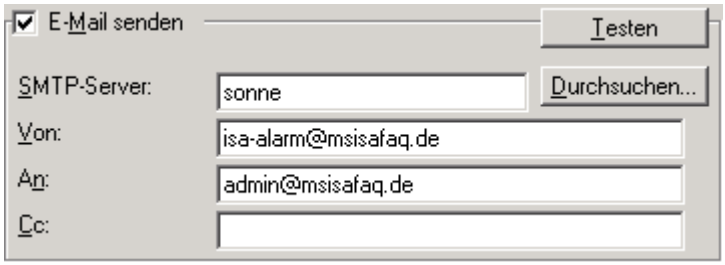
- Beliebiger ISA Server-Dienst
- ISA Server-Steuerungsdienst
- ISA Server-Firewalldienst
- ISA Server-Auftragsplanungsdienst

In der unteren Hälfte der Registerkarte werden weitere Eigenschaften des Alarms definiert. So wird hier zum Beispiel festgelegt, wie oft das oben ausgewählte Ereignis auftreten muss, bevor ein Alarm registriert werden soll. Die ist bei häufig auftretenden Ereignissen sinnvoll. So könnte z.B. ein einmal auftretendes SMTP-Filterereignis noch nicht beunruhigend sein. Wenn dieses Ereignis jedoch mehrmals pro Sekunde auftritt ist es eher meldenswert, da dann davon auszugehen ist, dass entweder ein unberechtigter Nutzungsversuch oder ggfs. ein Kommunikationsproblem zwischen den beteiligten Mailservern vorliegt.

Die letzte Registerkarte bietet verschiedene Möglichkeiten an, welche Aktion der ISA Server ausführen soll, wenn das definierte Ereignis eingetreten ist.



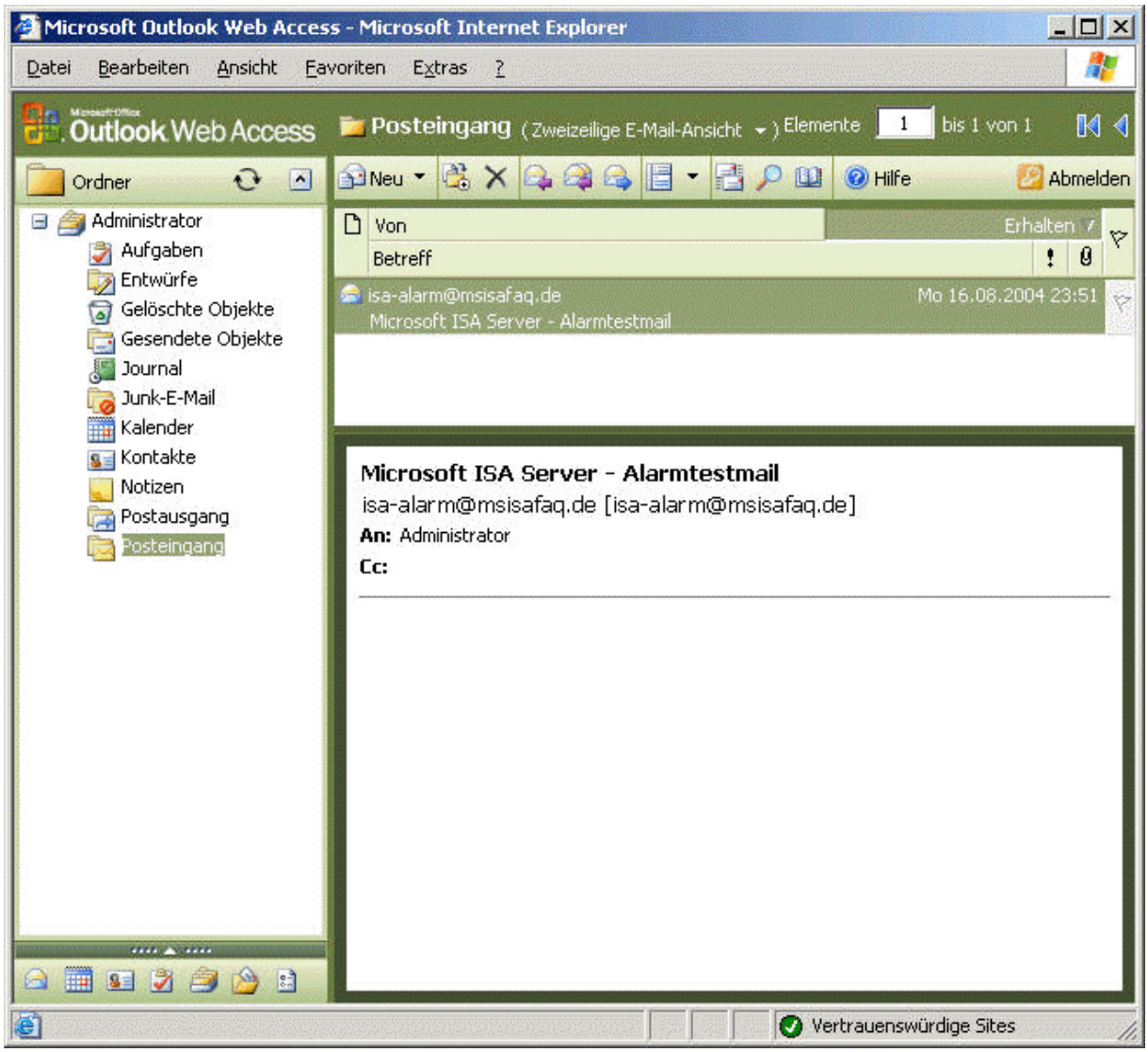
Eine der möglichen Aktionen ist, eine E-Mail zu versenden. Dazu müssen lediglich ein paar Angaben gemacht werden:



Tipp: Viele Mobilfunknetzbetreiber bieten Ihren Kunden eine individuelle Mailadresse an (z.B. Rufnummer@Provider.de. Damit lassen sich recht einfach wichtige Meldungen als SMS auf das Handy des Firewalladmins übertragen - vorausgesetzt natürlich, es besteht (noch) eine Internetverbindung und der Mailserver kann diese auch nutzen ;-)

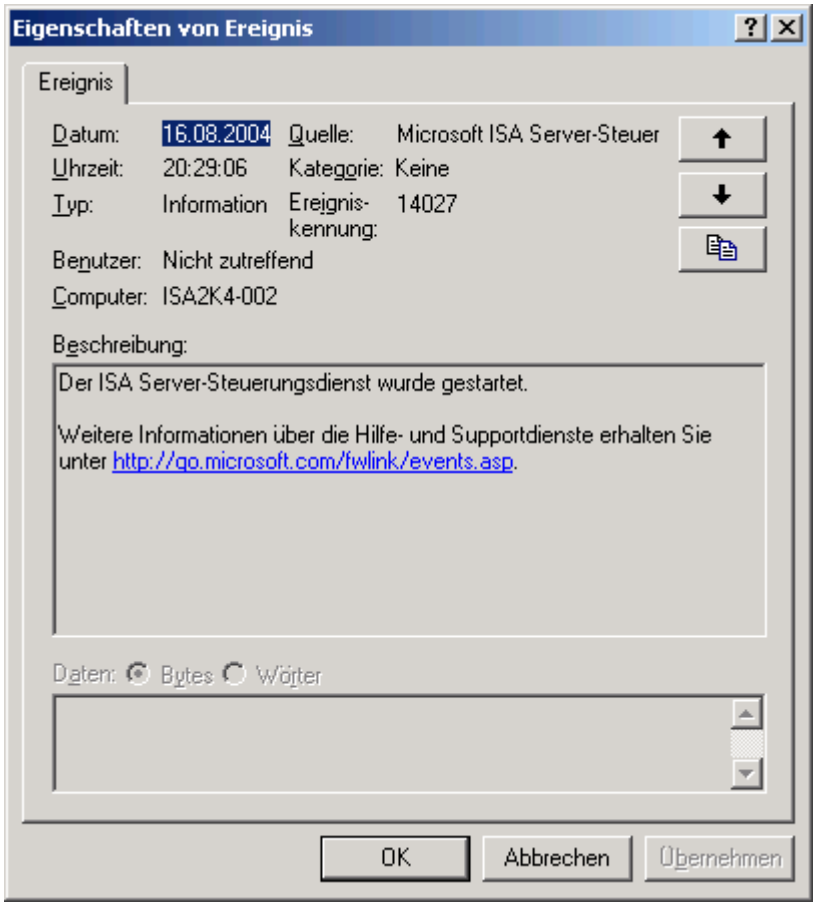
Durch eine Systemrichtlinie ist es dem ISA Server erlaubt, SMTP Verbindungen an interne Mailserver aufzubauen. Sofern diese Systemrichtlinie für Ihre individuellen Bedürfnisse nicht ausreichend ist kann sie erweitert oder durch eine zusätzliche Firewallrichtlinie ergänzt werden:

Über die Test-Funktion kann Überprüft werden, ob alle notwendigen Konfigurationen vorgenommen wurden. Wenn alles richtig ist, bekommt der Administrator aus dem Beispiel folgende E-Mail:



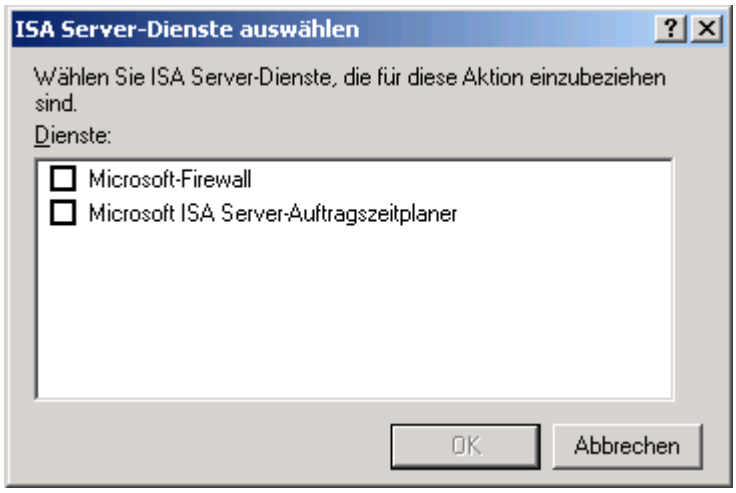
Zusätzlich zur oder statt der Mail-Benachrichtigung kann auch ein Programm (oder ein Script) ausgeführt werden, das wiederum verschiedene Aktionen startet. Wählen Sie dazu das Kontrollkästchen Programm aus und geben dann den an einer Eingabeaufforderung auszuführenden Befehl sowie das Konto ein, unter dem das Programm ausgeführt werden soll, wenn beim Auftreten der Alarmbedingung eine Anwendung ausgeführt werden soll.

Über die Option "In Windows-Ereignisprotokoll schreiben" wird das Ereignis im Eventlog des Computers protokolliert:



Zum Beenden des ISA Servers wählen Sie das Kontrollkästchen Ausgewählte Dienste beenden aus und klicken dann zur Auswahl der ISA Server-Dienste, die beim Auftreten der Alarmbedingungen beendet werden sollen, auf Auswählen.

An dieser Stelle können lediglich die folgenden beiden ISA Server-spezifischen Dienste ausgewählt werden:



Sollen andere Dienste gestoppt/gestartet werden als die vorgegebenen, besteht lediglich die Möglichkeit, dies per Batchfile oder Skript festzulegen und dies als Programm auszuführen.

Zum Starten von ISA Server wählen Sie das Kontrollkästchen Ausgewählte Dienste starten aus und klicken dann zur Auswahl der Dienste, die beim Auftreten der Alarmbedingungen gestartet werden sollen, auf Auswählen.

Vergessen Sie nicht, durchgeführte Änderungen noch zu Übernehmen:

In der ISA Server-Verwaltung wird die vollständige Liste aller vorgefallenen Ereignisse nach dem Alarmtyp sortiert angezeigt (Information, Warnung oder Fehler).

Im Dashboard ist eine Übersicht über den aktuellen Alarm-Zustand zu sehen:

Die Registerkarte Alarm zeigt dann nähere Details:

Durch die Auswahl des entsprechenden Alarmheaders können Sie eine ganze Gruppe von Alarminstanzen zurücksetzen. In der Alarmansicht werden Alarminstanzen der Kategorie entsprechend in Gruppen zusammengefasst (zum Beispiel Dienst heruntergefahren). Sie können die Gruppenheader erweitern oder reduzieren und so die enthaltenen Elemente anzeigen oder ausblenden.

Mithilfe der ISA Server-Verwaltung können Sie durch das Bestätigen von Ereignissen anzeigen, ob Sie ein spezifisches Ereignis oder eine Gruppe von Ereignissen bearbeiten. Wenn Sie ein Ereignis (oder eine Gruppe von Ereignissen) als anerkannt markieren, wechselt der Status der entsprechenden Ereignisse in der Alarmansicht, und diese Ereignisse werden nicht mehr in der Übersichtsansicht angezeigt.

Auf die gleiche Weise können Sie einen Alarm zurücksetzen, was zur Folge hat, dass er aus der Alarmansicht entfernt wird.

Hinweis: Gehen Sie mit den Alarm-Benachrichtigungen sorgfältig und bedächtig um. Es empfiehlt sich z.B. nicht, jedes Ereignis sofort als Mail zu versenden. In der Praxis kann es durchaus vorkommen, dass ein Server mehrere Dutzend PortScans am Tag aushalten muss. Wenn der Administrator darüber jedes mal eine Mail bekommt ist sein Postfach bald überfüllt und/oder der interne Mailserver streikt wegen Überlastung, obwohl er gar nicht das eigentliche Angriffsziel war.

Hinweis: Bei einem Neustart des ISA Server-Computers werden alle Alarme zurückgesetzt.

ISA Server 2004 – Protokollierung

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Im Artikel Übersicht Monitoring wurde eine Zusammenfassung aller Überwachungsfunktionen des ISA Server 2004 gegeben. Das vorliegende Kapitel beschreibt die Möglichkeit, die Protokollierungsfunktionen des ISA Server 2004 zu konfigurieren.

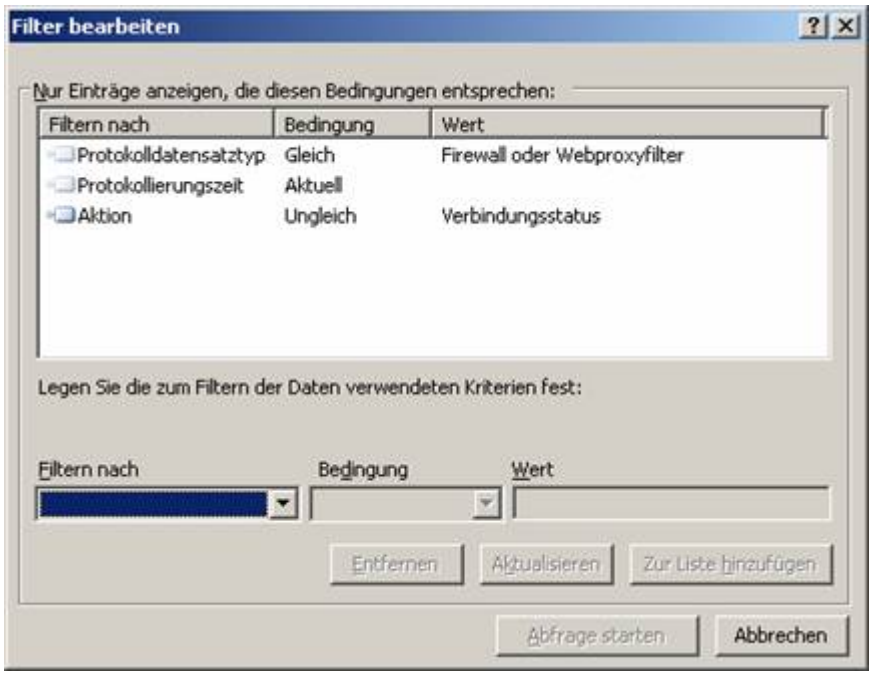
Einleitung

ISA Server 2004 protokolliert die Aktivität auf dem ISA Server-Computer. Diese Protokollierungen werden zum Erkennen von Sicherheitsverletzungen, zum Generieren von Berichten und zur Problembehandlung bei Netzwerkproblemen verwendet. Sie können festlegen, welche Informationen in den Protokollierungen in welchem der folgenden Formate gespeichert werden. Es stehen zur Auswahl:

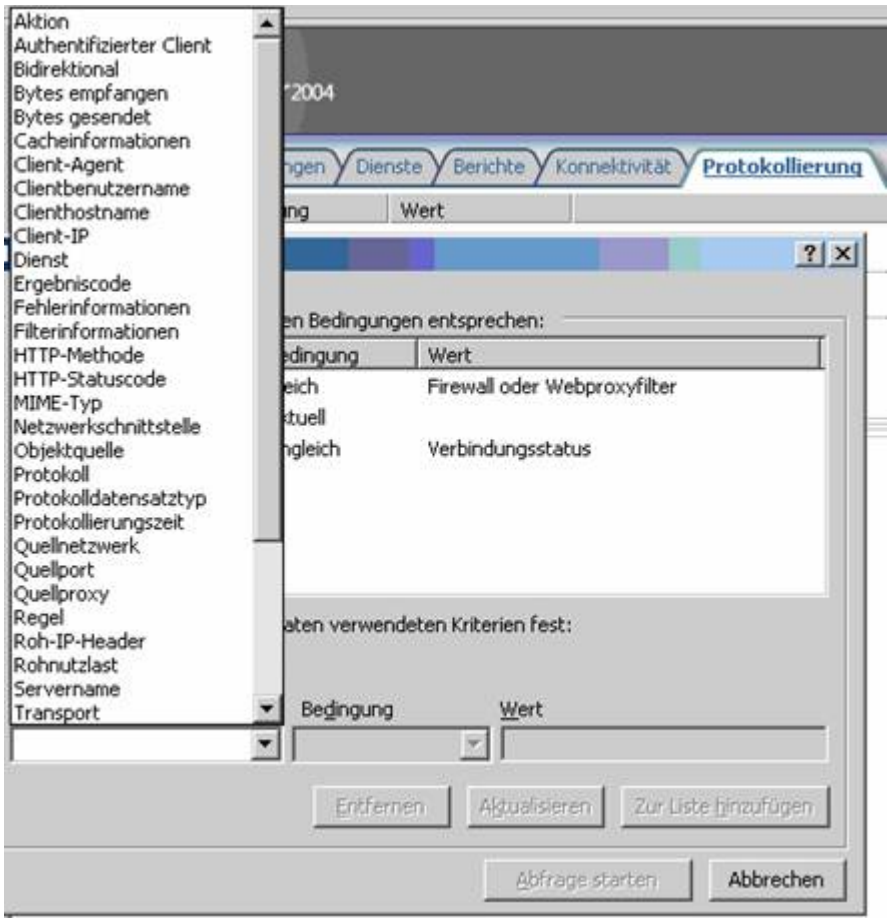
- Datei
- SQL
- MSDE

In der Protokollanzeige kann die Firewallprotokollierung und/oder die Webproxyprotokollierung angezeigt werden. Sie können die derzeit im Protokollrepository gespeicherten Onlineprotokollierungen anzeigen oder das Repository abfragen, um frühere Protokollierungen abzurufen. In beiden Modi können Sie Filter definieren, um die angezeigte Datenmenge zu begrenzen und übersichtlichere Auswertungen definieren zu können.

Der Standard Abfrage Filter filtert nach dem Protokolldatensatztyp = Firewall- oder Webproxyfilter, der Anzeige der Daten in Echtzeit und nach jedem Verbindungsstatus.

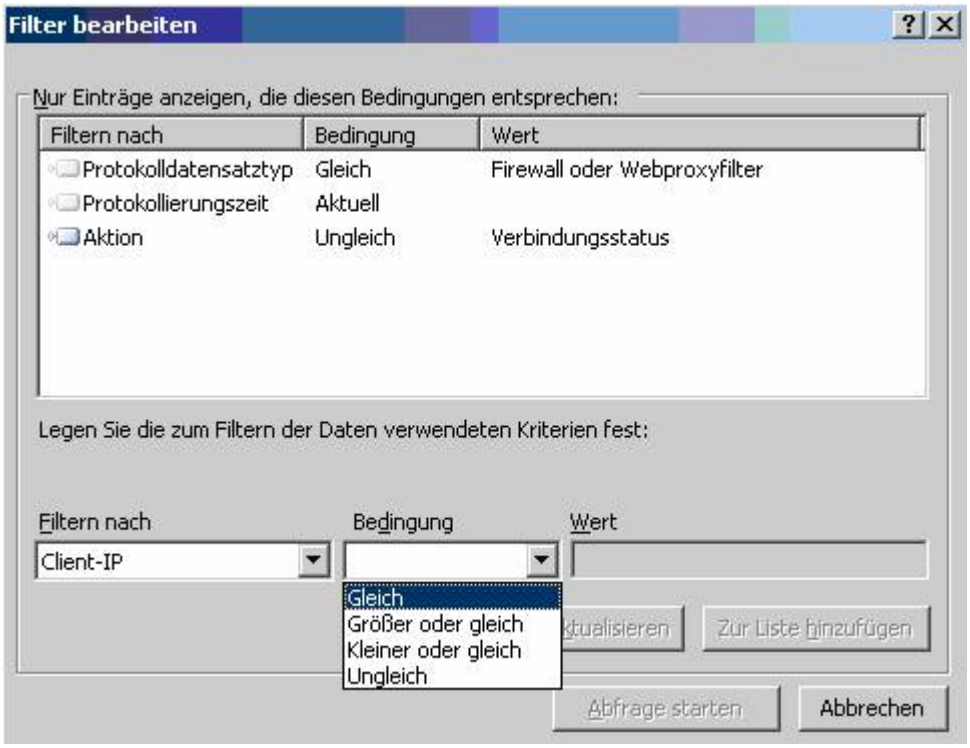


Sie können den Filter modifizieren, indem Sie im Standard-Filter unter *Filtern nach* den Filtertyp auswählen und dann anpassen. Sie können auch einen eigenen Filter erstellen, indem Sie unter Filtern nach einen Filter auswählen. Es stehen zahlreiche Filtermöglichkeiten zur Verfügung. Eine Übersicht über die Filtermöglichkeiten zeigt das nächste Bild.



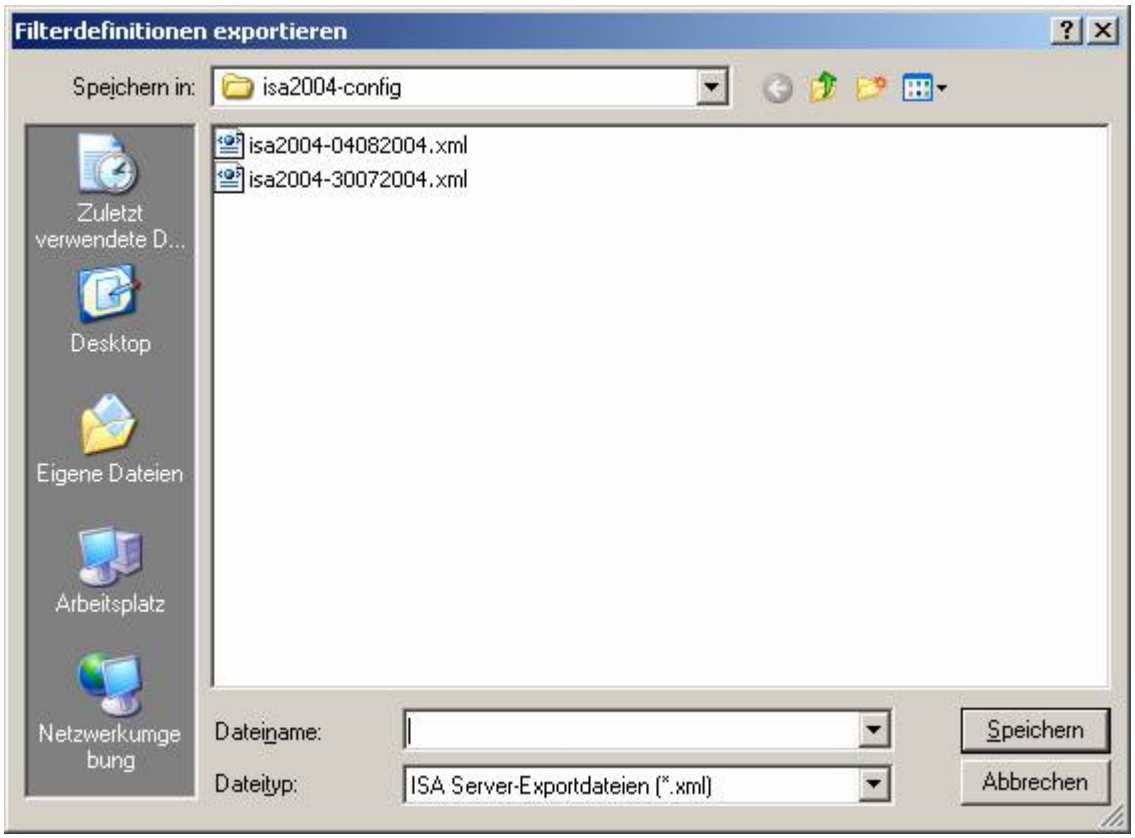
Nachdem Sie einen Filtertyp ausgewählt haben (in diesem Beispiel Client-IP) können Sie noch eine Bedingung zur Filterung hinzufügen.

Achtung: Die zur Verfügung stehenden Filter Bedingungen sind immer abhängig von der Filterart (Filtern nach). In diesem Beispiel ist die Filterart Client-IP und für diese Filterart stehen die Bedingungen Gleich, Größer oder gleich, kleiner oder gleich und Ungleich zur Verfügung.

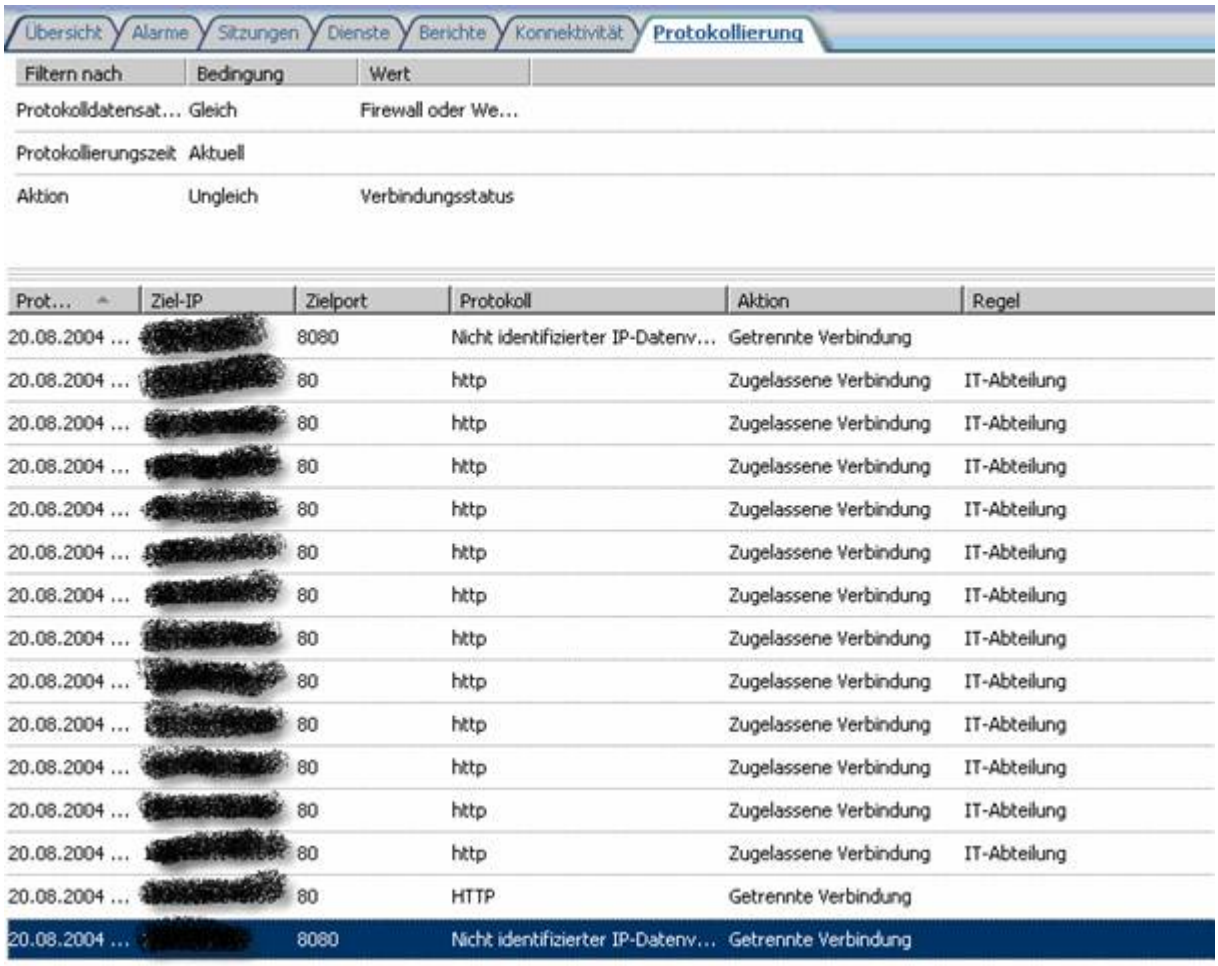


Als *Wert* wurde in diesem Beispiel die IP-Adresse 192.168.1.111 eingegeben. Zum Abschluss müssen Sie noch auf *Zur Liste hinzufügen* klicken, damit der neue Filter zur Filterbedingung hinzugefügt wird und auf *Abfrage starten* klicken.

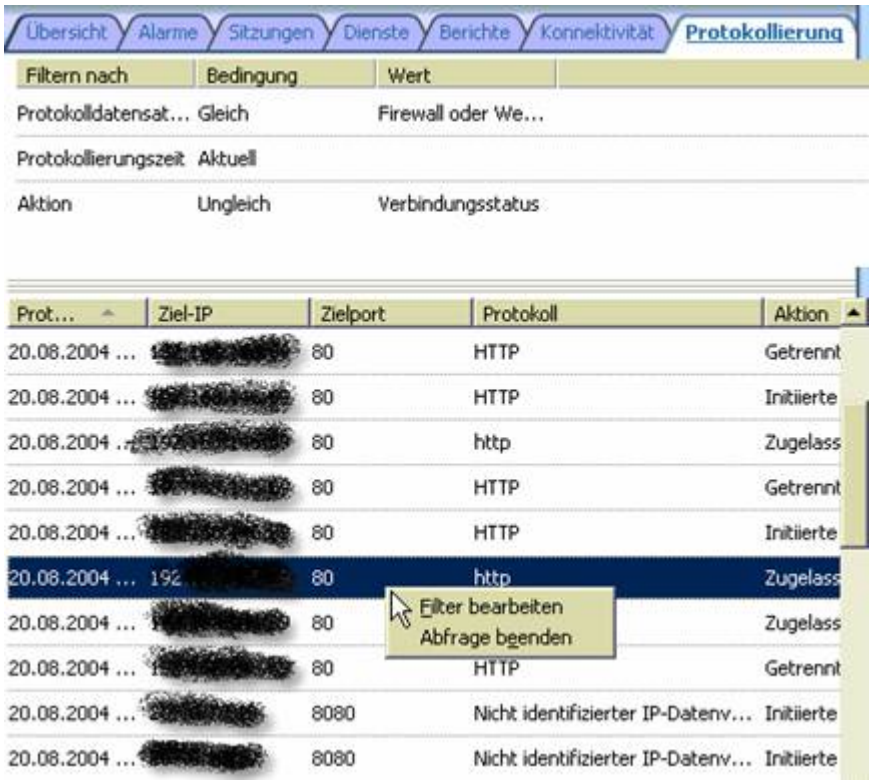
Einmal definierte Filteroptionen können exportiert und auch wieder importiert werden. Dieses Feature ist sehr hilfreich, weil sich der Administrator damit eine Sammlung an Filterdefinitionen erstellen kann, welche in einem bestimmten Verzeichnis gespeichert werden und dann bei Bedarf importiert werden können. Somit stehen dem Administrator fertige Vorlagen zur Verfügung mit welchem er die Protokolldaten filtern kann.



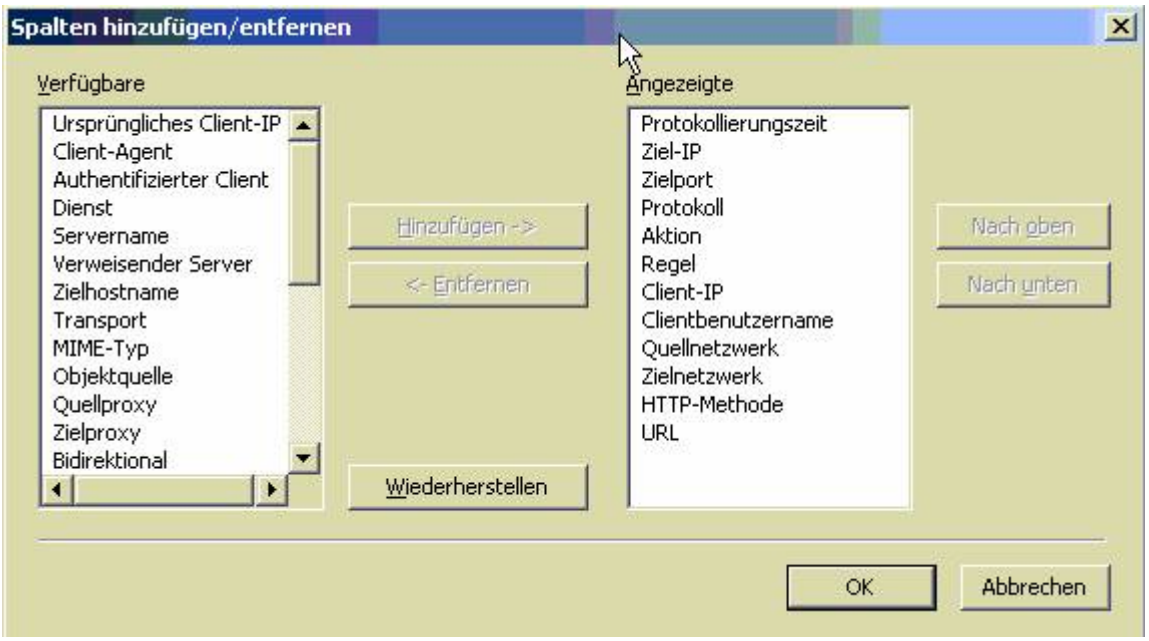
Der ISA Server 2004 zeigt jetzt in „Echtzeit“ die Protokolldaten, basierend auf Ihrer Filterdefinition an.



Mit einem Rechtsklick mit der Maus im Protokollfenster können Sie die *aktuelle Abfrage beenden* oder den *Filter bearbeiten.*



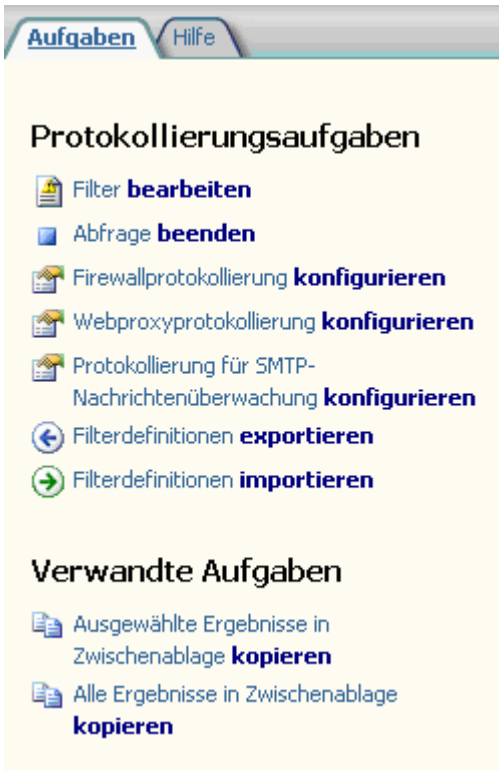
Sie können dem Protokollfenster zusätzliche Spalten Hinzufügen/Entfernen, sowie den Ursprungszustand *Wiederherstellen*.



Nachdem wir uns um die Anzeige der Protokolldaten und deren Filterung gekümmert haben, gehen wir jetzt zur Konfiguration der Protokollierung über. Der ISA Server 2004 bietet die Möglichkeit eine …

- Firewallprotokollierung
- Webproxyprotokollierung und
- SMTP Nachrichtenüberwachungsprotokollierung

einzurichten.



Folgende Protokollspeicherformate stehen zur Verfügung:

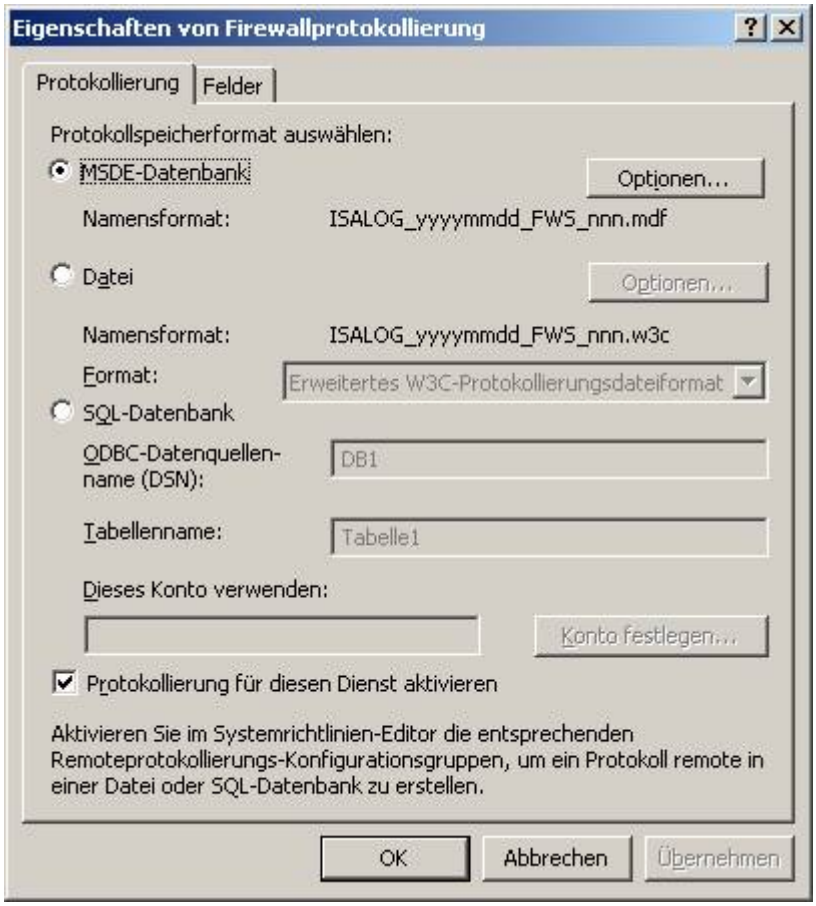
- MSDE-Datenbank
- Datei
  - W3C-Protokollierugsformat
  - ISA-Server Dateiformat
- SQL Datenbank über ODBC

Der Firewall- und Webproxydienst protokollieren die Daten per Default in eine MSDE Datenbank. Bei der MSDE (Microsoft SQL Server Desktop Engine) handelt es sich um eine kostenlose, funktionsreduzierte Datenbank aus dem Hause Microsoft. Für mehr Informationen über die MSDE sei auf folgende Webseite verwiesen: http://www.microsoft.com/sql/msde/

Bemerkung: Während der Installation des ISA Server 2004 wird eine MSDE Datenbank installiert.

Die SMTP Nachrichtenüberwachungsprotokollierung erfolgt per Default im erweiterten W3C Nachrichtenformat.

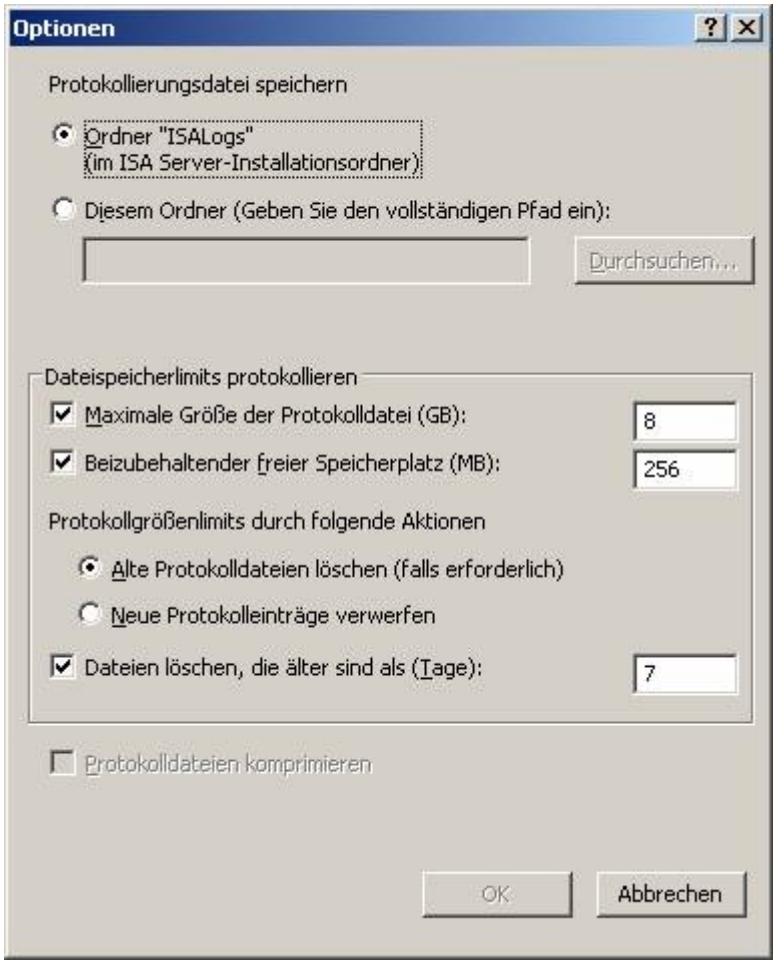
Im folgenden Bild sehen Sie die Möglichkeit das Protokollspeicherformat auszuwählen.



Achten Sie darauf, dass der Haken bei *Protokollierung für diesen Dienst aktivieren* aktiv ist. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden keine Ereignisse protokolliert.

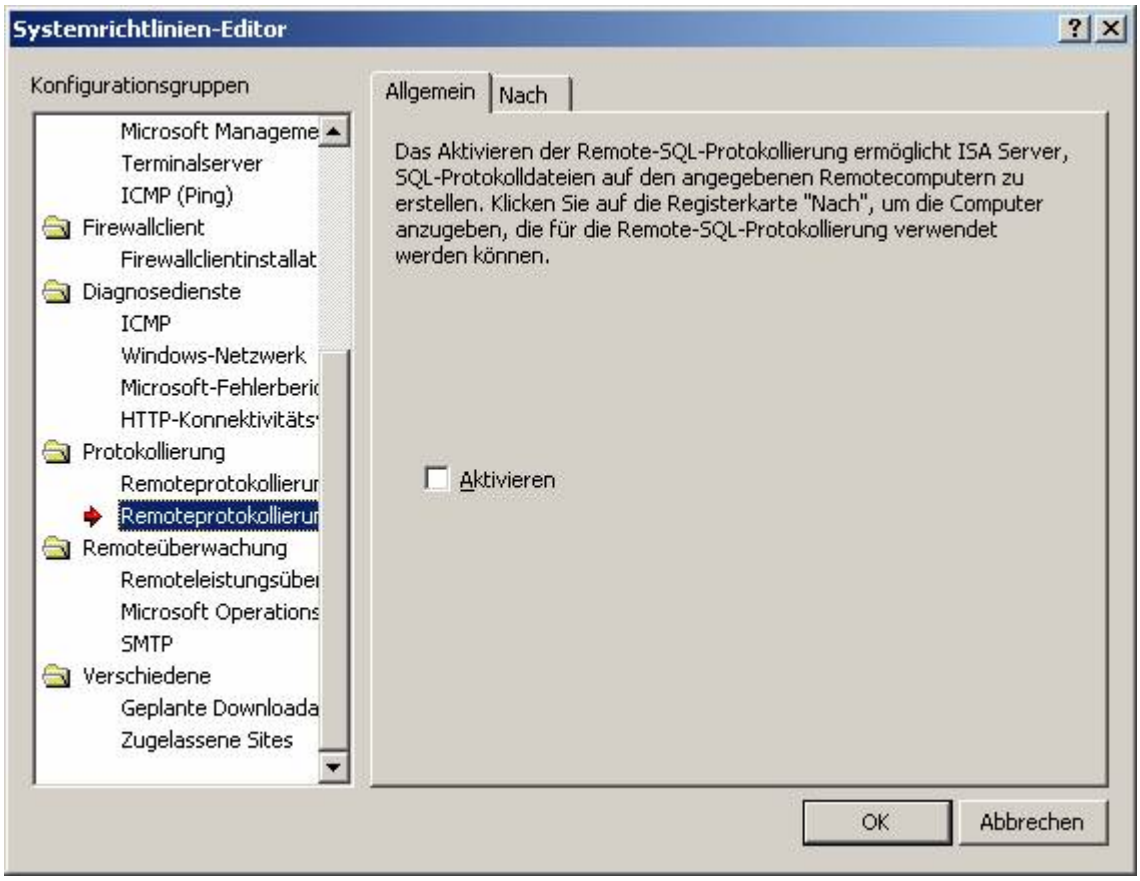
Sie können für die MSDE-Datenbank diverse Optionen konfigurieren. Es besteht die Möglichkeit, den Ort der Protokolldatei anzugeben, Dateispeicherlimits festzulegen und eine Aktion zu definieren, welche Aktion beim Erreichen des Protokollgrößenlimits durchgeführt werden soll.

Die maximale Protokolldateigröße bei der Verwendung der MSDE beträgt 8 GB. Insider sehen hier schon, dass es sich nicht um die Standard MSDE handelt, deren Größe auf maximal 2 GB limitiert ist, sondern um die erweiterte MSDE.



Die Protokolldateien können zur Reduzierung des Platzbedarfs komprimiert werden. Dieses Feature steht jedoch nur auf Partitionen mit dem NTFS Dateisystem zur Verfügung.

Wenn Sie eine Protokollierung in eine SQL Datenbank AUSSERHALB des ISA Server 2004 planen, müssen Sie mit Hilfe des Systemrichtlinien-Editor die *Remoteprotokollierung für SQL* Aktivieren und im Reiter *Nach* das Netzwerk angeben, welches den Remote SQL Server beinhaltet.


Systemrichtlinien-Editor
Konfigurationsgruppen
Microsoft Manageme
Terminalserver
ICMP (Ping)
Firewallclient
Firewallclientinstallat
Diagnosedienste
ICMP
Windows-Netzwerk
Microsoft-Fehlerberic
HTTP-Konnektivitäts
Protokollierung
Remoteprotokollierur
Remoteprotokollierur
Remoteüberwachung
Remoteleistungsüber
Microsoft Operations
SMTP
Verschiedene
Geplante Downloada
Zugelassene Sites
Allgemein
Nach
Das Aktivieren der Remote-SQL-Protokollierung ermöglicht ISA Server, SQL-Protokolldateien auf den angegebenen Remotecomputern zu erstellen. Klicken Sie auf die Registerkarte "Nach", um die Computer anzugeben, die für die Remote-SQL-Protokollierung verwendet werden können.
Aktivieren
OK
Abbrechen

ISA Server 2004 – System Hardening

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004
- Microsoft Windows Server 2003

Dieser Artikel beschreibt die notwendigen Schritte um einen installierten ISA Server 2004 so abzusichern, damit ein maximaler Schutz des ISA Servers und auch des darunter liegenden Betriebssystems gewährleistet ist. Es werden dabei nicht nur die Schritte erläutert, um einen ISA Server 2004 abzusichern, sondern auch Empfehlungen und Hinweise gegeben um für eine Gesamtsicherheit des Systems zu sorgen (sofern so etwas überhaupt möglich ist).

Dieser Artikel unterteilt sich in folgende Kapitel:

- Erstellen einer Security Policy
- Schulung des Personals + verantwortungsvoller Umgang mit den Firewallsystemen
- Physikalische Sicherheit
- Systemupdates für ISA und Windows
- Härten des Betriebsystems
- ISA Server 2004 Firewalltypen
- ISA Server 2004 Installationsmöglichkeiten
- Restriktives ISA Server Regelwerk
- Laufende Überwachung der Firewall
- Applikationen auf dem ISA Server
- Einsatz von Virenscannersoftware- und anderer Gateway-Software

Erstellen einer Security Policy

Die Erstellung und laufende Pflege einer Security Policy ist in vielen Unternehmen ein unliebsames Übel und wird gerne ignoriert, weil es, zugegebenermaßen, mit sehr viel Arbeit verbunden ist. Der Autor hält die Erstellung einer Security Policy in mittelständischen- und Großunternehmen jedoch für sehr sinnvoll.
Was ist eine Security Policy? - Eine SP definiert alle organisatorischen und technischen Maßnahmen eines Unternehmens welche zur Einrichtung, Betrieb und Wartung von Firewallsystemen notwendig sind. Die SP definiert nicht nur die technische Lösung und Dokumentation der Perimeter Sicherheit, sondern auch organisatorische Fragen wie Verpflichtungserklärungen der Mitarbeiter zum Datenschutz, Verhalten im Internet, aber auch Notfallpläne bei Kompromittierung des ISA Servers - Um nur ein Beispiel zu nennen: Sie sind Administrator eines mittelständischen Unternehmens mit 350 Beschäftigten, welches in hohem Maße von einer Internet Anbindung abhängig ist. jetzt stellen Sie fest, dass Sie einen "Eindringling" im System haben oder das System von Viren befallen ist. Können Sie jetzt einfach die Systeme vom Internet trennen? Wer entscheidet über die weitere Vorgehensweise? Diese und viele andere Fragen und Antworten werden in einer SP festgehalten.

Ein weiterer Vorteil einer SP ist natürlich auch, dass Sie damit eine ständig aktualisierte Dokumentation der Firewall-Infrastruktur besitzen.

Schulung des Personals + verantwortungsvoller Umgang mit den Firewallsystemen

Es kann nicht oft genug betont werden, wie wichtig es ist, für die Verwaltung des ISA Server und der umgebenden Infrastruktur qualifiziertes und geschultes Personal einzusetzen, welches sich nicht nur mit der Verwaltung des ISA Servers auskennt, sondern auch Verständnis für Netzwerkprotokolle, Systemsicherheit und allgemeine Sicherheitskenntnisse nachweisen kann.
Des weiteren ist ein verantwortungsvoller Umgang mit den Firewallsystemen notwendig. Eine unbewusste Fehlbedienung der Firewall kann zu unerwünschten Ergebnissen führen. Mehr zu diesem Thema erfahren Sie in dem Kapitel "*Restriktives ISA Server Regelwerk*".
Sollten Sie selbst nicht in der Lage sein, ein Firewallsystem wie den ISA Server 2004 zu verwalten, suchen Sie sich bitte entsprechende Unterstützung durch externes Consulting oder mit Hilfe der ISA Server Newsgroup und Webseiten wie dieser.

Jeder Anfang ist schwer, aber es ist auch noch kein Meister vom Himmel gefallen.

Physikalische Sicherheit

Für einen sicheren ISA Server Betrieb müssen Sie sich auch um die physikalische Sicherheit der Systeme kümmern. Unter den Begriff "Physikalische Sicherheit" fallen:

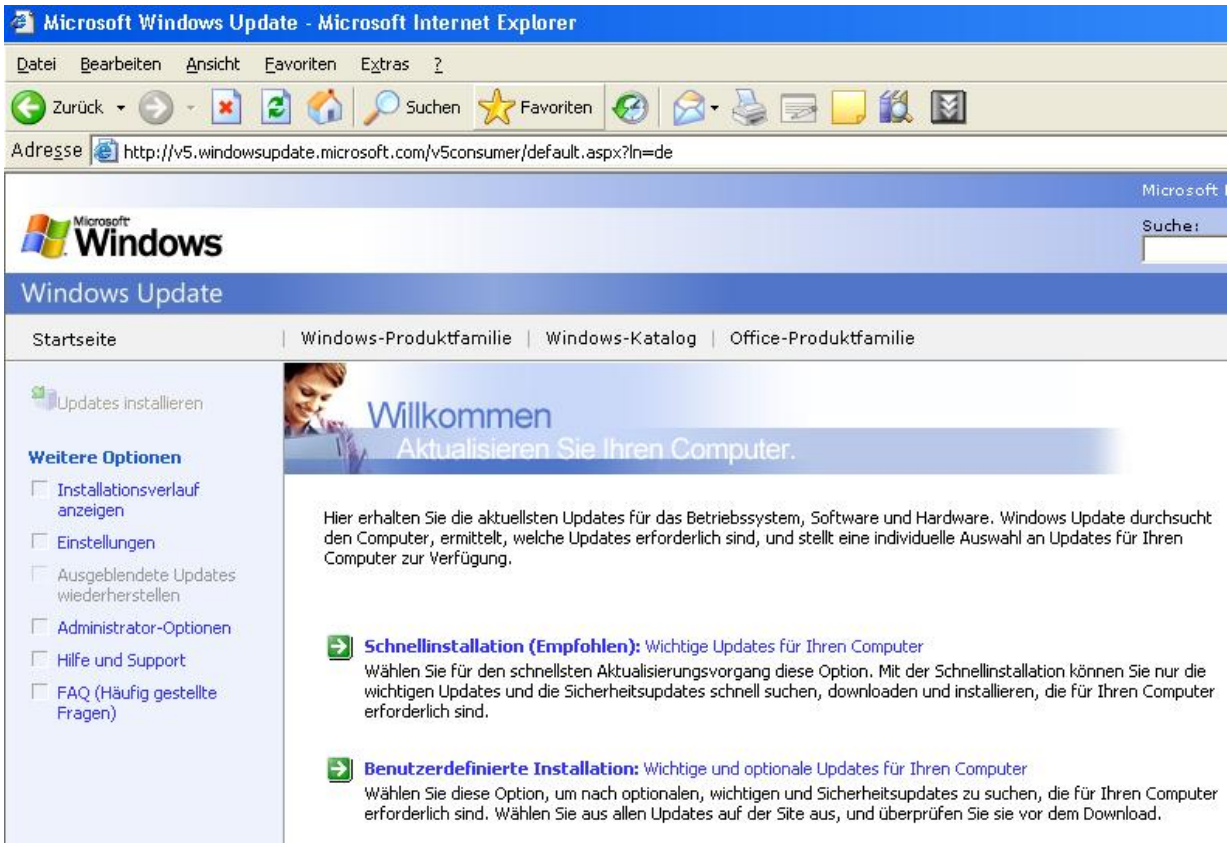
- Zugangsschutz zum Serverraum / IT-Infrastruktur (verstärkte Türen, Sicherheitsglas, Bewegungsmelder uvm.)
- Zutrittsschutz zum Serverraum / EDV-Raum (z. B. Zahlenschloss).
- Diebstahlschutz für die Server (zum Beispiel Montage in Racks mit abschließbaren Türen, spezieller Diebstahlschutz für Server)

Denken Sie auch daran, die restliche Infrastruktur entsprechend zu schützen. Es handelt sich hierbei natürlich nur um einige simple Beispiele. Das Thema "physikalische Sicherheit" kann Bände füllen.

Es gilt der Grundsatz: Kein System ist vor Angreifern sicher, wenn für den Angreifer ein physikalischer Zugriff auf die Systeme besteht.

Systemupdates für ISA und Windows

Der erste Schritt einer erfolgreichen Verteidigungslinie gegen potentielle Angriffe auf Ihre Infrastruktur ist die Überprüfung sowohl des ISA Servers als auch der Windows Plattform auf laufende Updates und neu entdeckte Sicherheitslücken. Stellen Sie ein sicher, dass Windows- und ISA Updates regelmäßig nach Prüfung eingespielt und dokumentiert werden.



Damit Sie bei potentiellen Sicherheitslücken auf dem laufenden sind, empfiehlt sich der regelmäßige Besuch der Microsoft Security Seiten und der Webseiten von Windows und ISA. Sie finden eine Übersicht über empfohlene Webseiten am Ende des Artikels.
Es besteht auch die Möglichkeit zum Abonnement von Newslettern, mit deren Hilfe Sie per E-Mail über neue Gefährdungen informiert werden.

Es lohnt sich auch ein regelmäßiger Blick auf die Webseite von www.msisafaq.de. Dieter Rauscher stellt auf dieser Seite eine Sammlung von Skripten zur Erstellung von HTTP Filter Signaturen zur Verfügung. Es handelt sich hier um Filter Signaturen diverses ISA Gurus.

Härten des Betriebsystems

Eine wichtige Aufgabe eines ISA Administrators ist es, das zugrunde liegende Betriebssystem (Windows 2000 oder Windows 2003) entsprechend abzusichern und auf die aktuellen Anforderungen abzustimmen. Ziel ist auch hier die Minimierung der Angriffsoberfläche. Maßnahmen zur Minimierung der Angriffsoberfläche:

- Deaktivierung nicht benötigter Dienste
- Installation nur der notwendigsten Windows Komponenten
- Einschränkung der administrativen Zugriffe
- Einsatz von Sicherheitsvorlagen

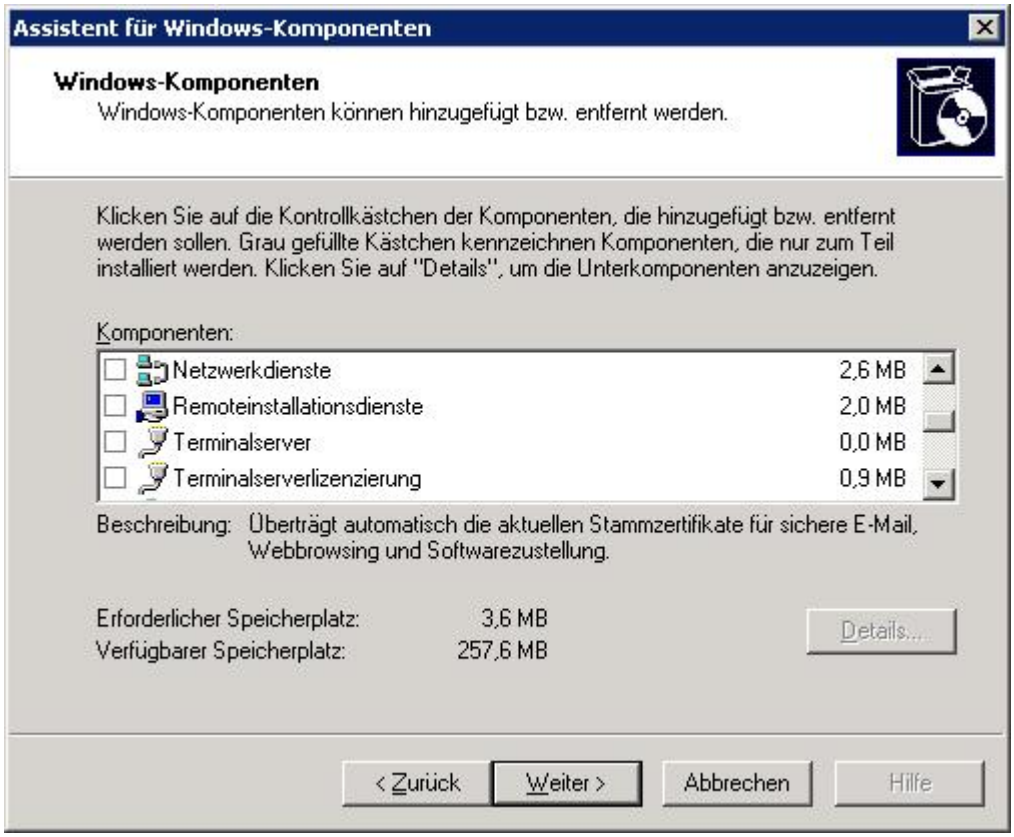
Deaktivierung nicht benötigter Dienste

Erforderliche Dienste um die Funktionalität des ISA Servers sicher zu stellen:

Dienstname	Funktionszweck	Startart
COM+ Event System	Betriebssystem	Manuell
Cryptographic Services	Betriebssystem (Sicherheit)	Automatisch
Event Log	Betriebssystem	Automatisch
IPSec Services	Betriebssystem (Sicherheit)	Automatisch
Logical Disk Manager	Betriebssystem (Festplattenmanagement)	Automatisch
Logical Disk Manager Administrative Service	Betriebssystem(Festplattenmanagement)	Manuell
Microsoft Firewall	Erforderlich für den ISA Server	Automatisch
Microsoft ISA Server Control	Erforderlich für den ISA Server	Automatisch
Microsoft ISA Server Job Scheduler	Erforderlich für den ISA Server	Automatisch
Microsoft ISA Server Storage	Erforderlich für den ISA Server	Automatisch
MSSQL$MSFW	Erforderlich für MSDE Logging am ISA Server	Automatisch
Network Connections	Betriebssystem(Netzwerkinfrastruktur)	Manuell
NTLM Security Support Provider	Betriebssystem (Sicherheit)	Manuell
Plug and Play	Betriebssystem	Automatisch
Protected Storage	Betriebssystem (Sicherheit)	Automatisch
Remote Access Connection Manager	Erforderlich für den ISA Server	Manuell
Remote Procedure Call (RPC)	Betriebssystem	Automatisch
Secondary Logon	Betriebssystem (Sicherheit)	Automatisch
Security Accounts Manager	Betriebssystem	Automatisch
Server	Erforderlich für ISA Server Firewall Client Share	Automatisch
Smart Card	Betriebssystem (Sicherheit)	Manuell
SQLAgent$MSFW	Erforderlich für MSDE Logging am ISA Server	Manuell
System Event Notification	Betriebssystem	Automatisch
Telephony	Erforderlich für den ISA Server	Manuell
Virtual Disk Service (VDS)	Betriebssystem (Festplattenmanagement)	Manuell
Windows Management Instrumentation (WMI)	Betriebssystem (WMI)	Automatisch
WMI Performance Adapter	Betriebssystem (WMI)	Manuell

Installation nur der notwendigsten Windows Komponenten

Installieren Sie auf der Windows Maschine nur benötigte Komponenten und verzichten Sie auf zusätzliche Programme wie DHCP, WINS, RIS, Terminalserver usw. wenn diese nicht absolut notwendig sind.



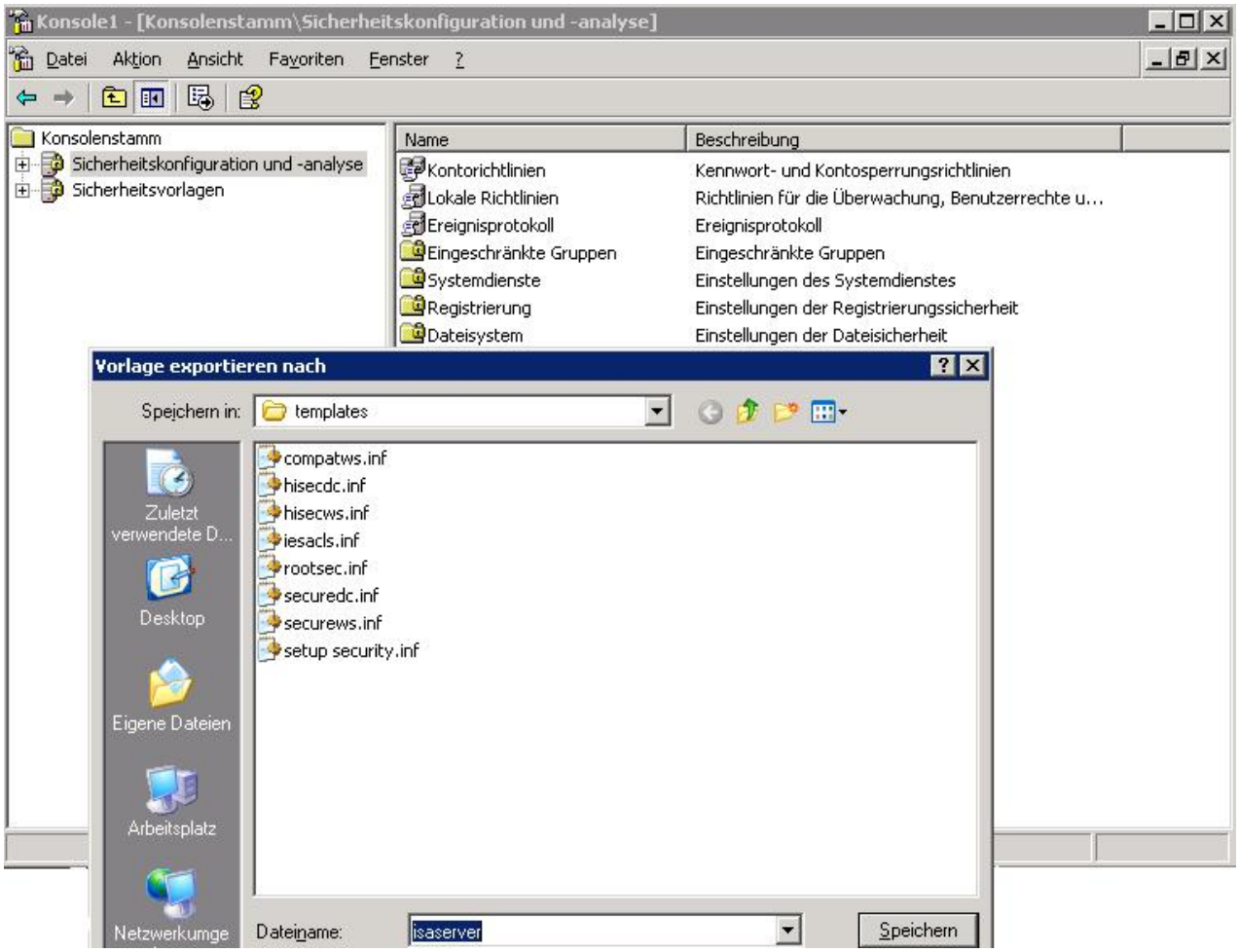
Einschränkung der administrativen Zugriffe

- Benennen Sie den Administrator Account nach erfolgter Windows Installation um und deaktivieren Sie den Account. Es kann sinnvoll sein, diesen Account dauerhaft zu monitoren, um zu ermitteln, wer versucht, sich mit dem Administrator Account anzumelden bzw. zu "hacken".
- Erstellen Sie einen zusätzlichen Account mit administrativen Berechtigungen, welchem Sie ein sehr langes und sicheres Kennwort vergeben.
- Reduzieren Sie ihre tägliche Arbeit am ISA Server mit administrativen Berechtigungen auf Minimum und verwenden Sie Administrator Privilegien nur, wenn das absolut notwendig ist.
- Beschränken Sie die Zahl der auf der Maschine eingerichteten Windows Administratoren auf ein Minimum.

Einsatz von Sicherheitsvorlagen

Ein bewährtes Prinzip zur Sicherung einer Windows 2000 / 2003 Maschine nach einem festen Schema sind so genannte Sicherheitsvorlagen. Sicherheitsvorlagen sind strukturierte Textdateien (.INF Dateien) die als Basis für eine Sicherheitskonfiguration mit dem Security Configuration Editor (SCE) verwendet werden können.
In den Sicherheitsvorlagen werden Einstellungen wie Kontenrichtlinien, Überwachungsrichtlinien, Registrierungseinstellungen, Konfiguration für Systemdienste uvm.

definiert. Nach erfolgter Definition können Sie das aktuelle System anhand der Sicherheitsvorlage konfigurieren. Mit Hilfe der Sicherheitsvorlage ist sichergestellt, dass Sie immer ein und dieselbe Sicherheitskonfiguration auf Ihre Systeme anwenden.



ISA Server 2004 Firewalltypen

ISA Server 2004 bietet die Konfiguration von verschiedenen Firewalltypen. Die Konfiguration basiert auf so genannten Netzwerkvorlagen. ISA Server 2004 bietet folgende Netzwerkvorlagen an:

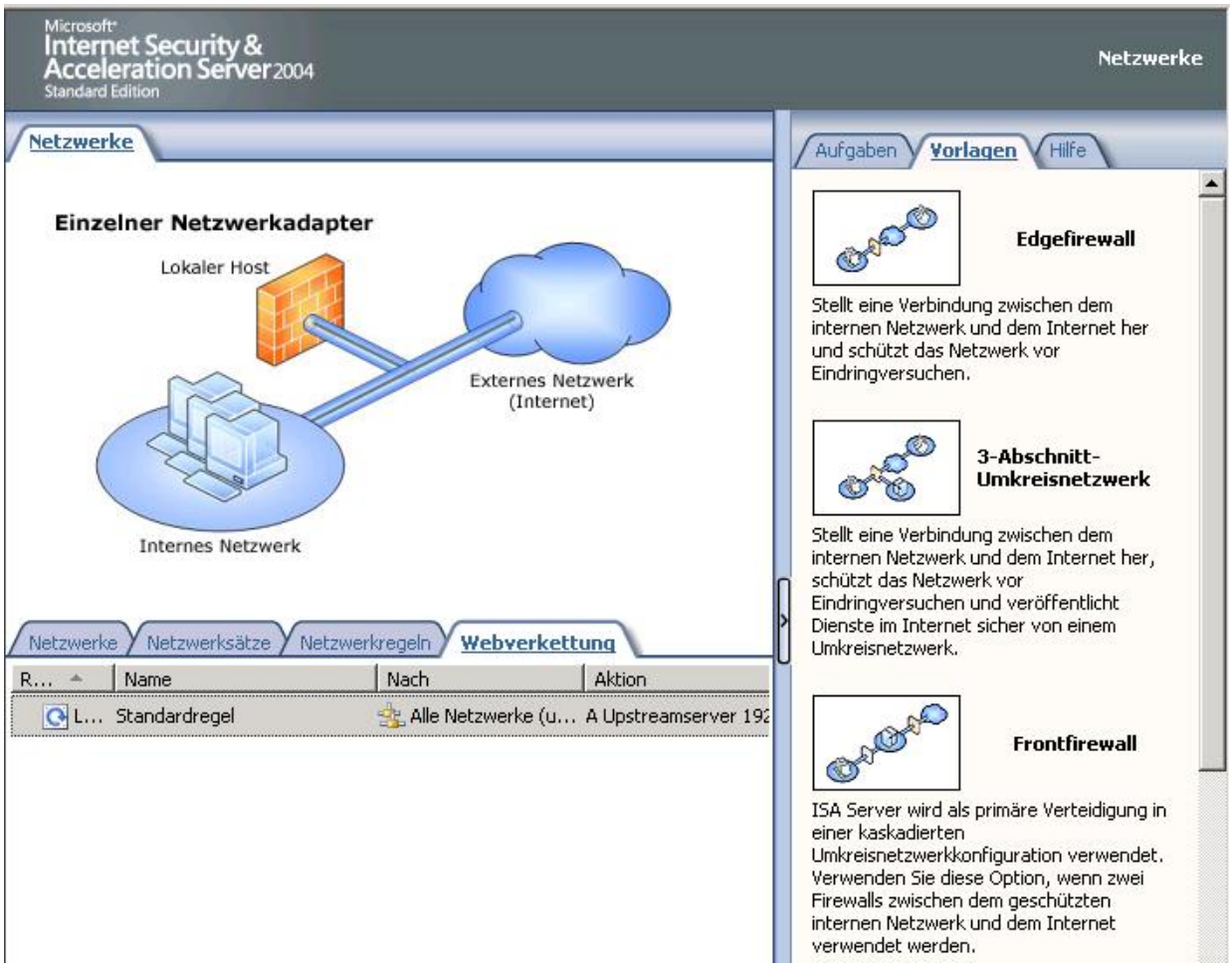
Edgefirewall
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle des Netzwerks befindet. Ein Netzwerkadapter ist hierbei mit dem internen Netzwerk verbunden. Der andere Netzwerkadapter verfügt hingegen über eine Verbindung mit einem externen Netzwerk (Internet). Bei Auswahl dieser Vorlage können Sie den gesamten ausgehenden Datenverkehr zulassen oder den ausgehenden Datenverkehr einschränken, so dass nur der Webzugriff gestattet wird.

3-Abschnitt-Umkreisnetzwerk
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server mit dem internen Netzwerk, dem externen Netzwerk und einem Umkreisnetzwerk (auch als DMZ, demilitarisierte Zone oder abgeschirmtes Subnetz bezeichnet) verbunden ist.

Frontfirewall-Netzwerkvorlage
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle eines Netzwerks befindet und zum Schutz des internen Netzwerks ein weiterer Firewall am Back-End konfiguriert ist.

Backfirewall-Netzwerkvorlage
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server an der Schnittstelle zwischen einem Umkreisnetzwerk und dem internen Netzwerk eingesetzt wird und zum Schutz des internen Netzwerks am Back-End ein weiterer Firewall konfiguriert ist.

Einzelner Netzwerkadapter
Bei dieser Vorlage wird eine Netzwerkkonfiguration mit einem einzelnen Netzwerkadapter angenommen, der sich innerhalb eines Umkreis- oder Firmennetzwerks befindet. In dieser Konfiguration dient ISA Server als Webproxy- und Cacheserver.



Für weitere Informationen zum Thema Netzwerkdefinition lesen Sie folgenden Artikel.

ISA Installationsmöglichkeiten

ISA Server 2004 lässt sich auf Windows 2000 und Windows 2003 installieren. Aufgrund der erweiterten Sicherheitsfunktionen und des etwas eingeschränkten Funktionsumfangs des ISA Servers unter Windows 2000 empfiehlt der Autor die Installation des ISA Servers auf einer Windows 2003 Maschine.
Bei der Installation des ISA Servers stellt sich des öfteren die Frage, wie die Windows 2000 /

2003 Maschine an das interne Netzwerk angebunden wird.

Es gibt hier zwei ultimative Aussagen:

- Installieren Sie den ISA Server 2004 **niemals** auf einem Windows 2000 / 2003 Domänencontroller
- Installieren Sie den ISA Server 2004 nicht auf einem Windows 2000 / 2003 Mitgliedsserver wenn sich der ISA Server als so genannte Frontfirewall oder auch Egde Firewall direkt mit dem "Internet" verbunden ist.

Microsoft empfiehlt auch in einigen Whitepapern die Installation der ISA Server 2004 in einem separaten Forest. Diese Konstellation macht aus Sicht des Autors erst Sinn, wenn man eine Vielzahl von ISA Servern betrieben will und zum Beispiel von Gruppenrichtlinien und der Speicherung der Array Informationen im Active Directory (nur ISA 2004 Enterprise) profitieren will.

Keine Regel ohne Ausnahme:

Betreiben Sie den ISA Server im Rahmen einer Front- und Backend Firewallkonfiguration als Backend-Server, bestehen keine Sicherheitsbedenken, den ISA Server 2004 auf einem Windows 2000 / 2003 Mitgliedsserver zu installieren.
Lässt Ihr IT Budget keine Investition in zusätzliche Hardware und Software-Lizenzen zu, können Sie den ISA Server natürlich auf einem Domänencontroller installieren (Microsoft geht mit dem Small Business Server 2003 ja diesen Weg).

Installieren Sie den ISA Server 2004 erst, nachdem Sie das zugrunde liegende Windows System entsprechend "gehärtet" haben. Installieren Sie den ISA Server von einer vertrauenswürdigen Installationsquelle, welche garantiert virenfrei ist und von deren Herkunft Sie sicher sind, dass es sich um die Original ISA Installationsdateien handelt.
Schließen Sie die Windows Maschine, auf der ISA Server 2004 installiert werden soll, nicht an das "Internet" an, bis Sie den ISA Server 2004 vollständig installiert, konfiguriert und die notwendigen Updates installiert haben. Nach erfolgter ISA Installation existiert eine Default Policy, die so genannte Cleanup Rule, welche sämtlichen Datenverkehr zum Internet verweigert.

Restriktives ISA Server Regelwerk

Stellen Sie als ISA Server Administrator sicher, dass Sie mit einem minimalen ISA Server Regelwerk arbeiten, welches nur das absolute Mindestmaß an Firewallrichtlinien zulässt.

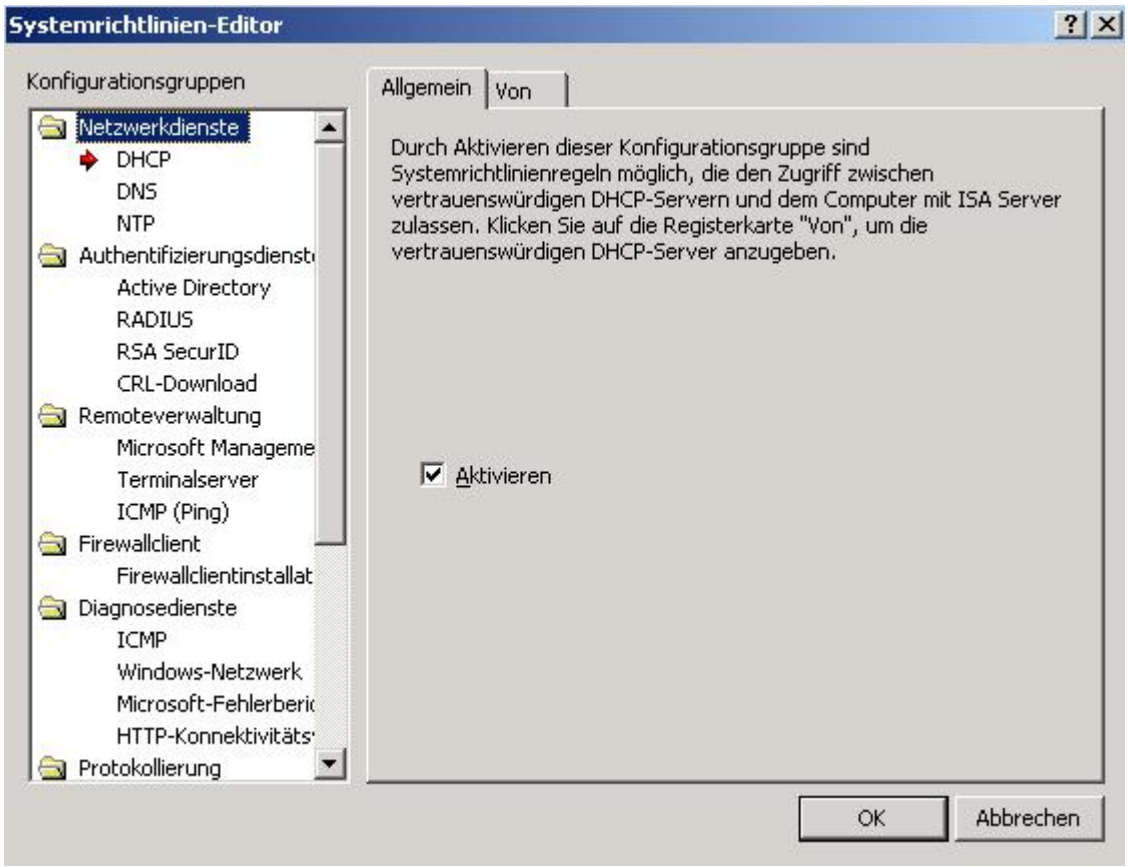
Faustformel: Bei der Einrichtung eines Firewallregelwerkes wird nach dem Minimalprinzip gearbeitet.

Gehen Sie dazu wie folgt vor:

Verschaffen Sie sich einen Überblick über Ihre Infrastruktur und protokollieren Sie die notwendigen Kommunikationsbeziehungen von **INTERN** nach **EXTERN** und zum **ISA Server** selbst.
Legen Sie fest, welche Kommunikationsbeziehungen von **EXTERN** nach **INTERN** notwendig sind.
Basierend auf diesen Informationen gehen Sie dazu über, die notwendigen Protokolle zu

definieren (wenn Sie der ISA Server noch nicht vorkonfiguriert hat), erstellen Sie die notwendigen Computersätze, Zielsätze usw.

Modifizieren Sie jetzt als erstes die Systemrichtlinie des ISA Servers, um diese auf Ihre Bedürfnisse anzupassen. Microsoft liefert mit dem ISA Server 2004 eine Standard Systemrichtlinie aus, welche den Zugriff auf das interne Interface des ISA Servers schützt und nur bestimmte Infrastrukturprotokolle wie DNS, DHCP usw. zulässt. Passen Sie diese Systemrichtlinie auf Ihre aktuelle Konfiguration an um eine geringstmögliche Angriffsfläche zu bieten.



Jetzt können Sie die entsprechenden Regelwerke erstellen und dokumentieren. Dokumentieren Sie jede erstellte Firewall Policy mit dem Erstellungsgrund und was diese Policy ermöglichen soll, damit Sie auch in naher Zukunft einen Überblick über Ihr Regelwerk behalten. Beachten Sie auch die Reihenfolge der Firewall Policies. ISA Server 2004 arbeitet die Firewall Policies anders als der ISA Server 2000 ab.

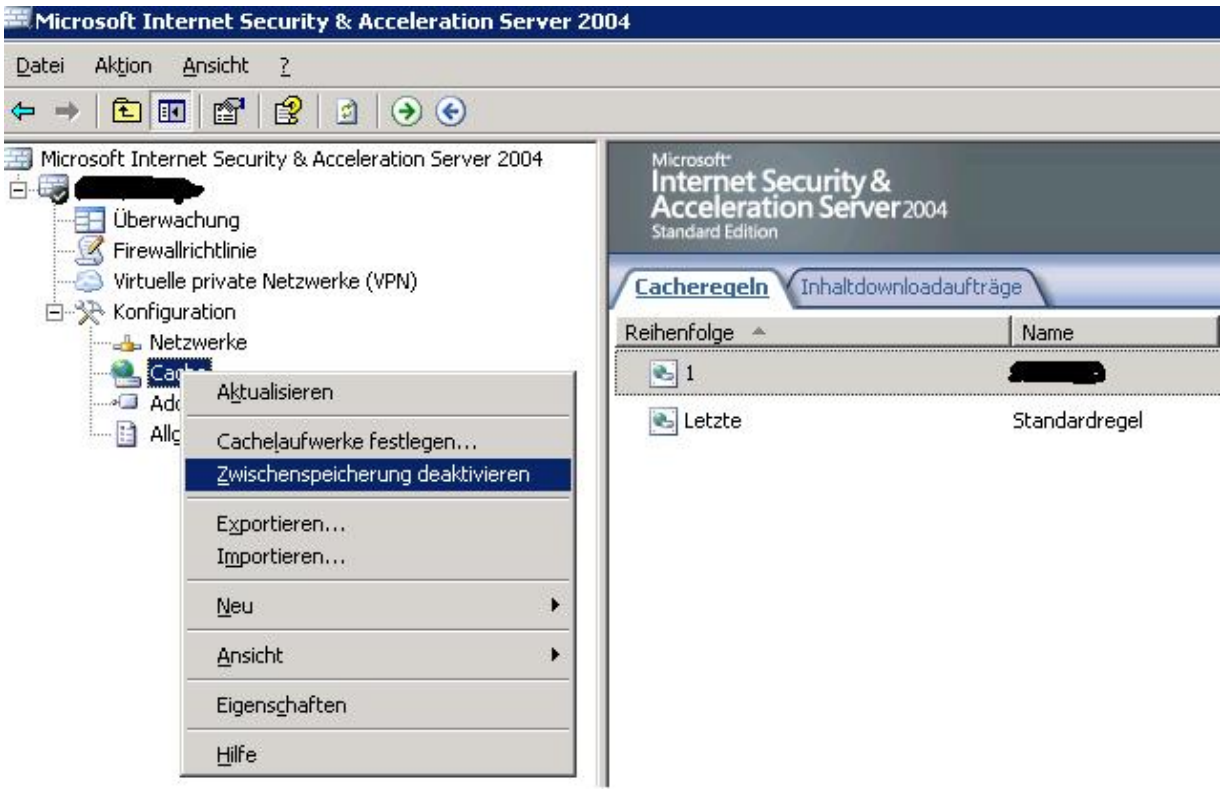
Kleiner Tipp:

Platzieren Sie die am häufigsten verwendeten Firewall Policies am Anfang des Regelwerkes um die Performance etwas zu erhöhen. Achten Sie aber trotzdem darauf, dass durch das Verschieben der Regeln keine unerwünschten Ergebnisse auftreten.

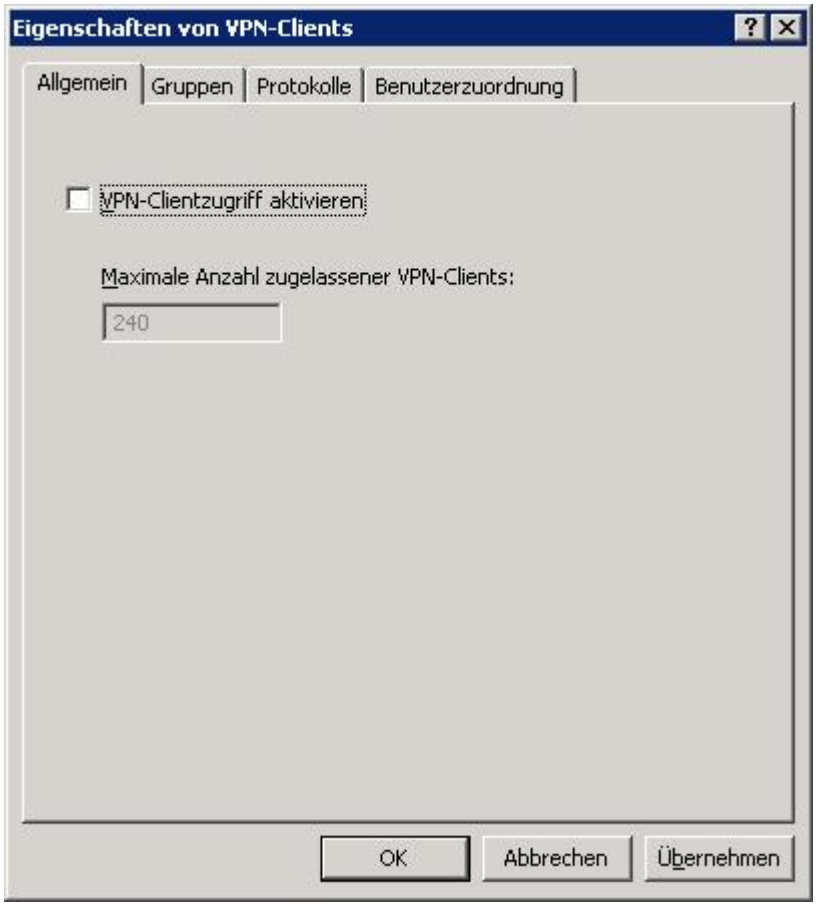
Arbeiten Sie nach dem Minimalprinzip, dass heißt, erstellen Sie das Regelwerk so restriktiv und minimal wie möglich.

Aktivierte ISA Server Komponenten

Je nach Einsatzzweck des ISA Server 2004, sollten Sie nur die absolut notwendigen ISA Komponenten während der Installation auswählen und auch nach der Installation nur die benötigten Komponenten aktivieren.
Benötigen Sie zum Beispiel den ISA Server nicht als Webcache Lösung, lassen Sie den Cache deaktiviert (Default Einstellung des ISA Server 2004).



Verwenden Sie den ISA Server 2004 nicht als VPN Server, so können Sie die VPN Funktionalität am ISA Server 2004 auch deaktivieren.



Deaktivieren Sie auch nicht benötigte Anwendungs- und Webfilter.

ISA Server Verwaltungsdelegation

ISA Server 2004 bietet als erste Microsoft Firewall die Möglichkeit, an nicht administrative

Benutzer ISA Berechtigungen zu delegieren. Es stehen drei verschiedene Verwaltungsdelegationen zur Verfügung:

- ISA Server-Standardüberwachung
- Erweiterte ISA Server-Überwachung
- ISA Server-Hauptadministrator

ISA Server-Standardüberwachung

Benutzer und Gruppen mit dieser Rolle können die Computer- und Netzwerkaktivität des ISA Server-Computers überwachen, ohne jedoch einzelne Überwachungsfunktionen konfigurieren zu können.

Erweiterte ISA Server-Überwachung

Benutzer und Gruppen mit dieser Rolle können sämtliche Überwachungsaufgaben (einschließlich der Konfiguration von Protokollen und Alarmdefinitionen) sowie alle für die Rolle ISA Server-Basisüberwachung verfügbaren Überwachungsfunktionen durchführen.

ISA Server-Hauptadministrator

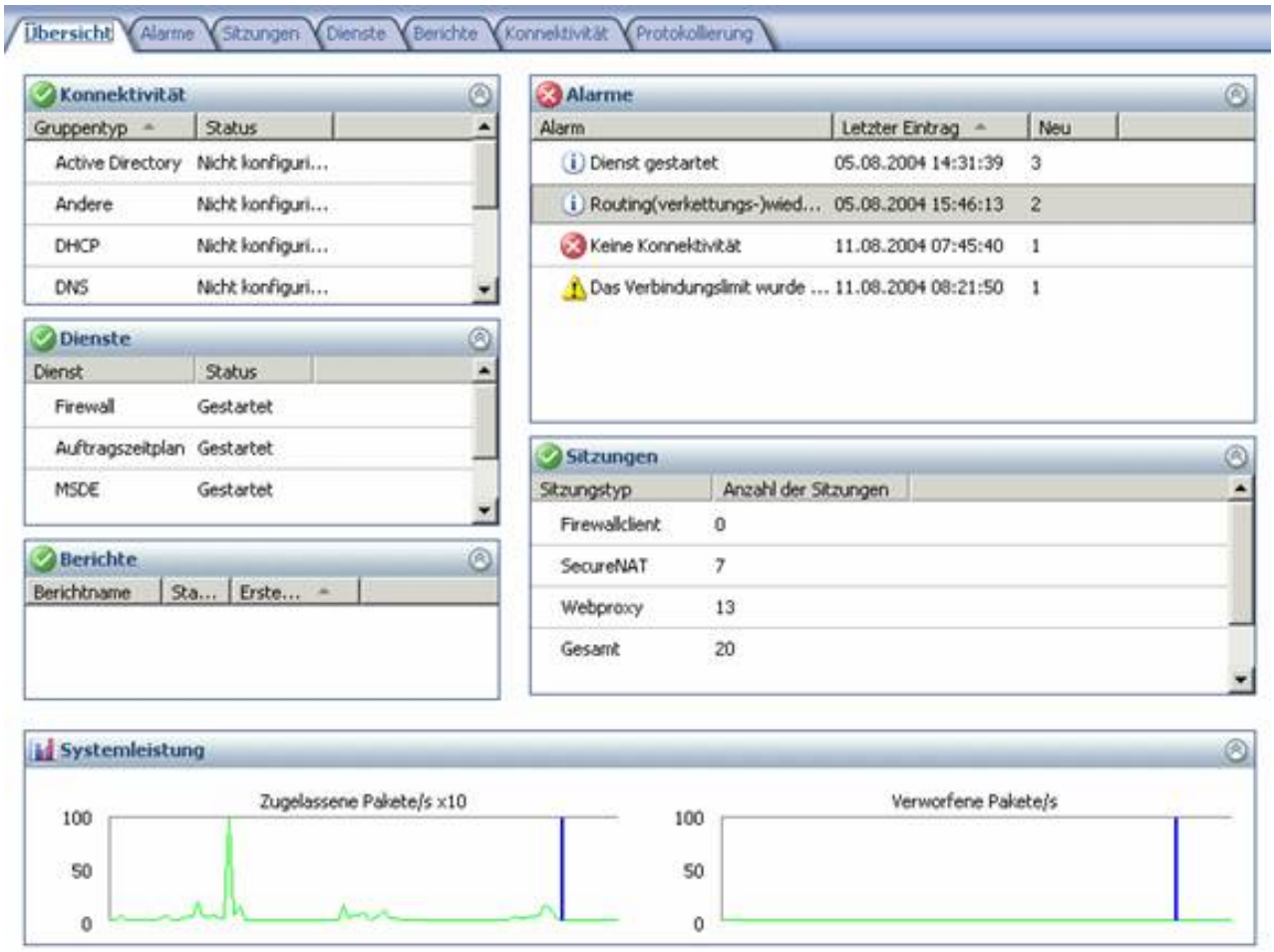
Benutzer und Gruppen mit dieser Rolle können sämtliche ISA Server-Aufgaben durchführen, einschließlich des Anwendens von Netzwerkvorlagen, der Netzwerk- und Regelkonfiguration und der Überwachung.

Laufende Überwachung der Firewall

Als ISA Server Administrator ist es Ihre ureigenste Aufgabe, das Firewallsystem ständig überwachen und für eine ausreichende Performance zu sorgen.

Zu den Überwachungs/Wartungstätigkeiten gehören:

- Tägliche Analyse der ISA Server Logdateien auf verdächtige Aktivitäten
- Tägliche Durchsicht der Meldungen der Ereignisanzeige
- Überprüfen der Festplattenkapazität um einen Systemüberlauf zu vermeiden
- Sichern der Logdateien und der Ereignisanzeige auf einen anderen Rechner als den ISA Server um im Falle eine Angriffs Logmanipulation vorzubeugen und eine gewisse Revisionssicherheit bei Protokolldaten zu erreichen.



Für weitere Informationen zum Thema Monitoring lesen Sie folgenden Artikel und diesen.

Lassen Sie sich auf alle Fälle bei dem Eintreten von wichtigen Ereignissen auf dem ISA Server informieren. Es stehen Ihnen dazu verschiedene Möglichkeiten zur Verfügung:

Sie können sich zum Beispiel per E-Mail informieren lassen, wenn ein bestimmter ISA Alarm auftritt.

Für weitere Informationen zum Thema ISA Alarme lesen Sie folgenden Artikel.

Applikationen auf dem ISA Server

Sehr häufig wird die Frage gestellt, wie man denn bestimmte Applikationen auf dem ISA Server installiert und diese dann zur Nutzung von internen und auch externen Zugriffen konfiguriert.

Es gibt hier eine definitive Aussage: **Eine Firewall ist eine Firewall und kein Applikationsserver!**

Was heißt das konkret? Im Normalfall ist der ISA Server eine reine Firewall und es sind keine Applikationen auf dem ISA Server installiert, weil diese die Sicherheit der Firewall kompromittieren können und das System offener für so genannte Exploits machen. Vermeiden Sie nach Möglichkeit die Installation von Anwendungen direkt auf dem ISA Server. Installieren Sie statt dessen Applikationen, welche im Internet zugänglich sein sollen, in der DMZ (DeMilitarisierten Zone). Sie können auch interne Server über ISA Server 2004 Serververöffentlichungs- und Webserververöffentlichungsregeln verfügbar machen.

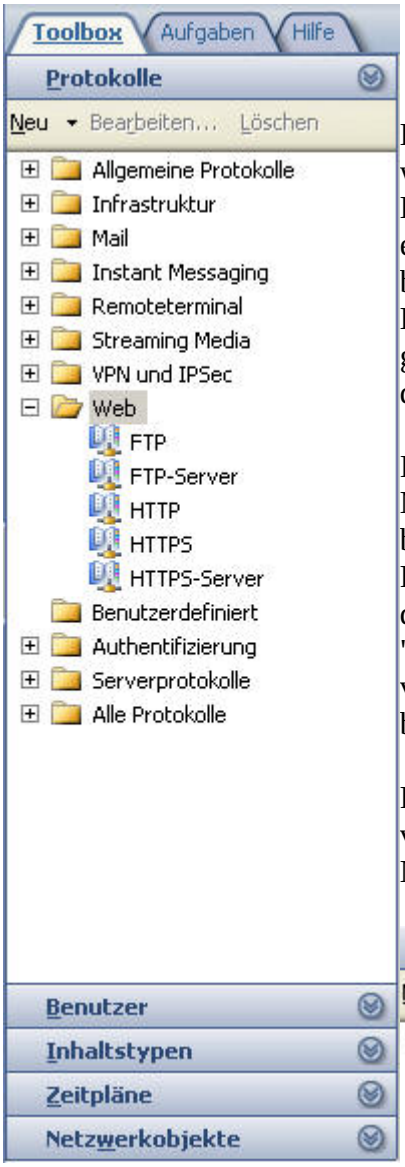
Einsatz von Virenscanner- und anderer Gateway-Software

Fast schon obligatorisch zu erwähnen ist es, dass Sie auf dem ISA Server 2004 einen sich ständig aktualisierenden Virenscanner installieren, welcher das System laufend auf Virenbefall überprüft. Es existieren eine Vielzahl von Virenscannerlösungen für den ISA Server.
Da der ISA Server den Einstiegspunkt in Ihr Firmennetzwerk darstellt, gilt der Grundsatz: "Stoppen Sie Eindringlinge und Viren so früh wie möglich". Aus diesem Anlass installieren Sie auf dem ISA Server auch Content Management Systeme, Intrusion Detection Systeme (IDS) und Gateway basierte Virenscanner, welche sämtlichen Datenverkehr von **EXTERN** nach **INTERN** auf Virenbefall, schadhaften Code, ausführbaren Dateien uvm. durchsucht und basierend auf Ihrer festgelegten Policy verweigert, bzw. überprüft.
Es stehen eine Vielzahl von Third Party Produkten für den ISA Server 2004 zur Verfügung. Klicken Sie hier für eine Anbieter Übersicht.

Toolbox - "Werkzeugkasten" für Firewallrichtlinien

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004



Eine Firewallrichtlinie regelt grob gesagt, von wo nach wo wer wann welche Verbindung aufbauen darf. Man kann es wie Kuchen backen betrachten - man benötigt viele Zutaten, damit eine leckere Torte entsteht. Ok, eine Firewallrichtlinie ist nicht besonders schmackhaft, verglichen mit einer Schwarzwälder Kirschtorte. Dennoch ist es sehr wichtig, genau und wirklich nur genau die notwendigen Zutaten zu verwenden. Und genau um diese Zutaten (oder: Werkzeuge) geht es in diesem Artikel.

Im Vergleich zum ISA Server 2000 wurde die Managementkonsole wesentlich erweitert und verbessert. Satt bisher unterschiedlichen (und unübersichtlichen) Knoten für Protokolldefinitionen, Zeitplänen, Clientadresssätzen etc. wurde die Toolbox eingeführt. In dieser Toolbox sind sämtliche "Zutaten" für Firewallrichtlinien enthalten. Neben den bereits vordefinierten Elementen können natürlich auch eigene benutzerdefinierte Elemente erstellt werden.

Für viele häufig benutzen Protokolle sind Protokolldefinitionen vorhanden. Ebenso können Zeitpläne, Benutzer- oder Netzwerkobjekte erstellt oder vorhandene verwendet werden:

Wenn z.B. eine bestehende Firewallrichtlinie um ein weiteres Protokoll erweitert werden soll, kann dies per drag and drop erfolgen. Einfach das Protokoll auf die Regel ziehen.

Über das Toolbox-Menü können wie bereits angesprochen neue Elemente hinzugefügt werden:

Wenn ein bestehendes Element ausgewählt ist, kann es auch bearbeitet oder gelöscht werden. Dies gilt nicht für bereits systemseitig vorhandene Elemente.

Sollte die Toolbox nicht angezeigt werden, wenn Sie in der ISA Server Managementkonsole und darin den Knoten "Firewallrichtlinie" öffnen, kann es sein, dass sie verkleinert wurde. In diesem Fall befindet sich am rechten Rand Mitte ein Verschiebeelement. Damit kann die Toolbox nach links ausgeklappt werden.

Erstellen eines neuen benutzerdefinierten Protokollelementes in der Toolbox

---

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Im Artikel Toolbox wurde bereits der "Werkzeugkasten" vorgestellt, der beim Erstellen oder Verändern einer Firewallrichtline als Vorratsbehäter für die Bestandteile verwendet wird.

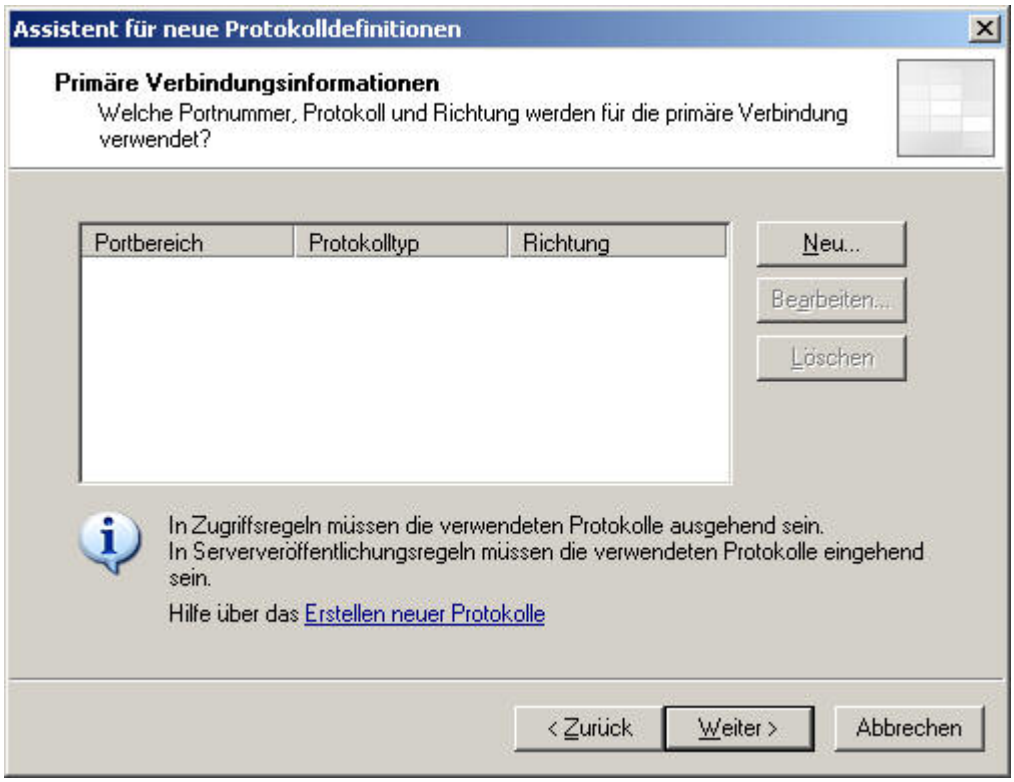
Dieser kurze Artikel hier beschreibt, wie ein neues Protokollelement (oder: Protokolldefinition) erstellt wird.

Im folgenden Beispiel wird ein Protokollelement für das T-Online ClassicGate erstellt, welches bereits hier für den ISA Server 2000 ausführlich beschrieben wurde.

In der ISA Server Managementkonsole findet man unterhab des Knotens "Firewallrichtlinie" auf der rechten Seite die Toolbox. Um dort ein neues Protokollelement zu erstellen muss in der Toolbox der Bereich Protokolle aufgeklappt werden. Dann im Menü Neu -> Protokoll auswählen.

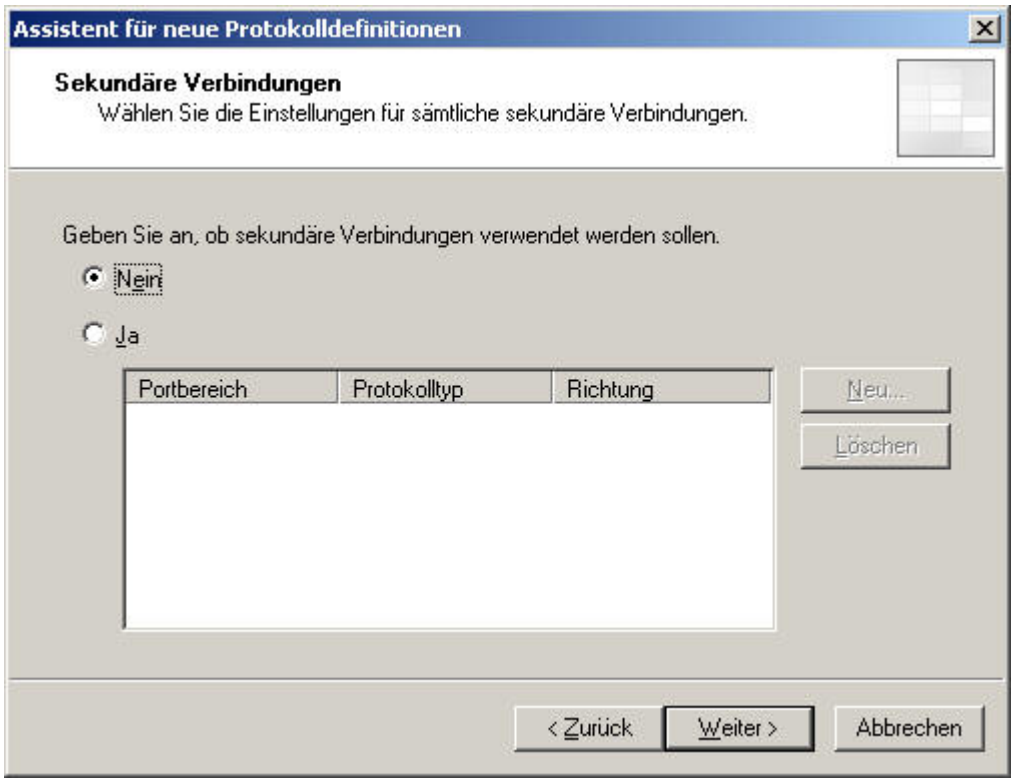
Für ein Protokoll sollte ein sprechender Name verwendet werden. Dies gilt übrigens nicht nur hierfür. Für sämtliche erstellten Objekte für die Konfiguration des ISA Servers (z.B.

Firewallrichtlinien) sollten klare Namen verwendet werden, die auf einen Blick eine Übersicht geben, was das jeweilige Element beinhaltet.



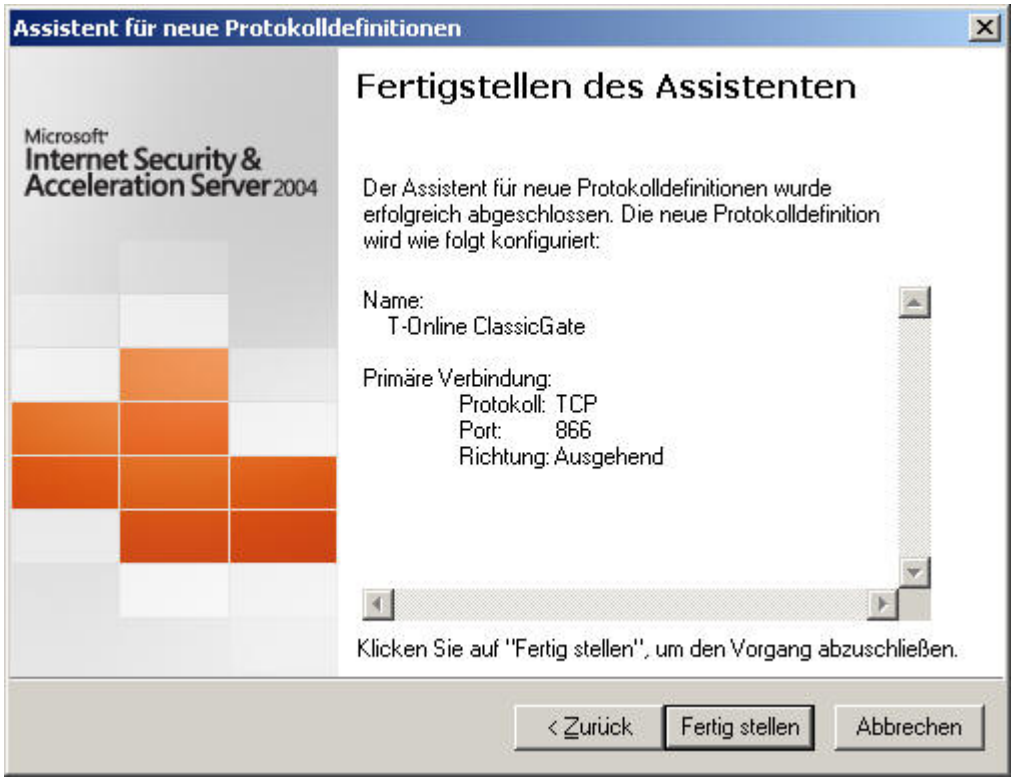
Die zweite Dialogbox bietet eine Übersicht der für dieses Protokollelement verwendeten/benötigten Ports und TCP/IP-Protokolle. Über den Button "Neu" gelangt man zu folgendem Fenster:

Für das T-Online ClassicGate wird TCP Port 866 ausgehend benötigt.

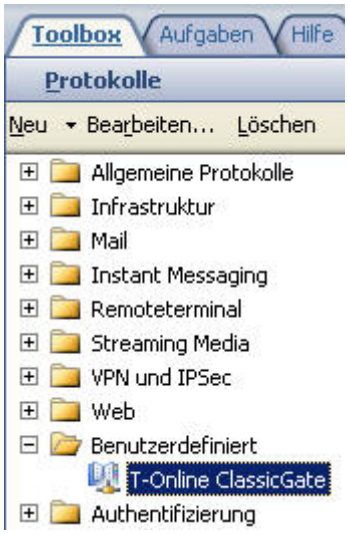


Sekundäre Ports werden in diesem Fall nicht benötigt. Sekundäre Ports werden von manchen Anwendungen benötigt, die über mehr als einen Port mit einem anderen System kommunizieren.

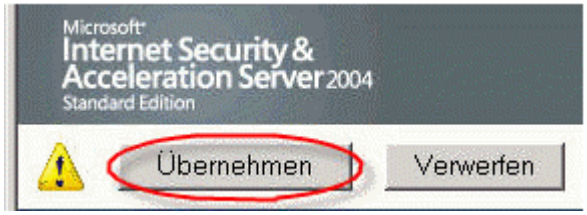
Das letzte Dialogfenster bringt eine kurze Zusammenfassung, die z.B. für Dokumentationszwecke verwendet werden kann (hier funktioniert copy&past):



Das nun neu erstellte Protokollelement wird n der Toolbox unter "Benutzerdefiniert" angezeigt:



Damit die Änderung bzw. die Neueinrichtung wirksam wird, muss die Konfiguration noch gespeichert werden:



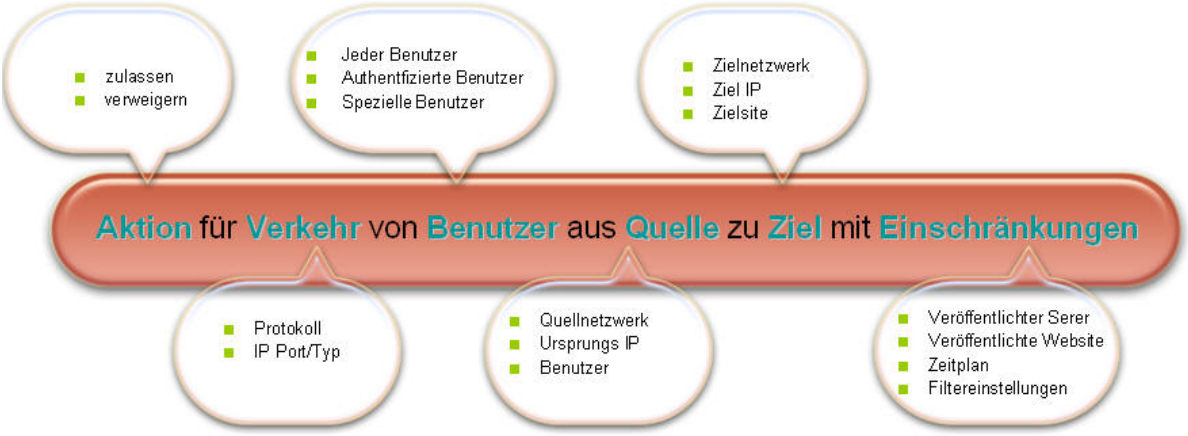
Firewallrichtlinien

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Eine Firewallrichtlinie regelt grob gesagt, von wo nach wo wer wann welche Verbindung aufbauen darf. Man kann es wie Kuchen backen betrachten - man benötigt viele Zutaten, damit eine leckere Torte entsteht. Ok, eine Firewallrichtlinie ist nicht besonders schmackhaft, verglichen mit einer Schwarzwälder Kirschtorte. Dennoch ist es sehr wichtig, genau und wirklich nur genau die notwendigen Zutaten zu verwenden. Niemand würde auf die Idee kommen, in diese Kirschtorte eine Flasche Cola hinzuzufügen. Und genauso sollte niemand auf die Idee kommen, Firewallrichtlinien zu weit zu öffnen und/oder Protokolle hinzuzufügen, die gar nicht benötigt werden. Die sinnloseste und gefährlichste Regel ist, allen Verkehr zuzulassen. Wer solche Regeln erstellt, hat möglicherweise nicht sonderlich viel von einem Firewallkonzept verstanden. Dem Thema "Firewallkonzept" ist ein eigener Artikel gewidmet.

Die Grafik unten verdeutlicht, wie eine Firewallrichtlinie aufgebaut ist und welche Komponenten zu welchen Bedingungen verwendet werden können.



Sehen wir uns die einzelnen **Elemente** etwas detaillierter an:

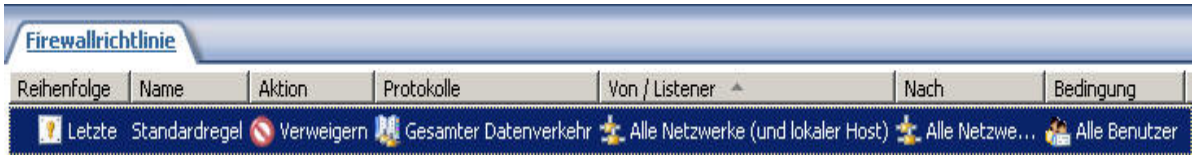
- **Aktion:** Eine Regel kann erlaubt (zugelassen) oder verboten (verweigert) werden. Beim Erstellen einer Richtlinie muss unbedingt darauf geachtet werden, dass sie von oben nach unten abgearbeitet werden. Wenn z.B. oben eine Regel existiert, die der Benutzerin Birgit die Nutzung von POP3 erlaubt und weiter unten eine Regel steht, die allen Benutzern POP3 verbietet hat Birgit dennoch Zugriff auf POP3.
- **Verkehr:** Die Regel kann entweder für ein IP-Protokoll (z.B. ICMP) oder einen TCP/UDP Port gültig sein.
- **Benutzer:** Hier kann angegeben werden ob die Regel nur für bestimmte (authentifizierte) Benutzer gelten soll.

- **Quelle:** Eine Regel muss definieren, von wo aus das zugelassene/verweigerte Protokoll genutzt werden kann. Der ISA Server 2004 unterstützt ein unbegrenztes (virtuelles) Netzwerkmodell. Es können also mehrere (virtuelle) Netzwerke definiert werden für unterschiedliche Zwecke. Zur Netzwerkdefinition ist ebenfalls ein Artikel verfügbar. Als Quellenangabe kann entweder ein ganzes Netzwerk, ein Netzwerkset, bestimmte Computersätze oder IP-Adressbereiche verwendet werden.
- **Ziel:** Das Ziel ist kann genauso wie die Quelle ein ganzes Netzwerk, ein Netzwerkset, bestimmte Computersätze oder IP-Adressbereiche enthalten. Hiermit wird festgelegt, wohin der zugelassene/verweigerte Verkehr aus der angegebenen Quelle hin darf. Um beim oben begonnen Beispiel von Birgit zu bleiben: Hier könnte festgelegt werden, dass Birgit nur einen bestimmten POP3-Server abfragen darf.
- **Einschränkungen:** Zum Schluss sollte noch die gerade erstellte Regel beschränkt werden. Hierzu stehen zum Beispiel Zeitpläne oder HTTP-Filtereinschränkungen zur Verfügung. Mit einem Zeitplan kann gesteuert werden, dass Birgit nur zwischen 09:00 und 18:00 Uhr einen bestimmten POP3-Server abfragen darf. Wenn die Richtlinie den Zugriff auf HTTP zulässt, kann in den HTTP-Filtereinstellungen beispielsweise konfiguriert werden, dass der MSN-Messenger nicht über HTTP eine Verbindung aufbauen darf. Wie das konfiguriert wird, beschreibt ein eigener Artikel.

Außer für "Aktion" können innerhalb einer Regel mehrere Elemente aus einer Kategorie (solange sie sich nicht gegenseitig ausschließen) verwendet werden. So kann zum Beispiel mit Hilfe von unterschiedlichen Zeitplänen festgelegt werden, dass Birgit während der Arbeitszeit (die in einem Zeitplan von 08:00-12:00 und 13:00 bis 17:00 Uhr festgelegt wurde) und während der Mittagspause (von 12:00 bis 13:00 Uhr, definiert in einem zusätzlichen Zeitplan) POP3 nutzen darf.

Wer den ISA Server 2000 kennt, wird sich etwas umgewöhnen müssen. Der ISA 2000 kannte verschiedene Orte/Knoten innerhalb der Managementkonsole, an denen Richtlinien für den Zugriff (nach außen und/oder nach innen) erstellt und verwaltet wurden. Dies wurde in der aktuellen 2004er Version komplett verändert. Es gibt nur noch einen Ort für Richtlinien. Um genau zu sein, gibt es doch zwei Orte ;-) Es gibt einmal die Firewallrichtlinien und es gibt die Systemrichtlinien. Firewallrichtlinien regeln grundsätzlich den Verkehr zwischen den verschiedenen Netzwerken. Systemrichtlinien regeln alles, was der ISA Server selber für den Betrieb benötigt. Systemrichtlinien werden standardmäßig nicht angezeigt, können jedoch eingeblendet werden.

Direkt nach der Installation existiert bereits eine Firewallrichtlinie:



Diese Richtlinie kann (mit der Ausnahme der Protokollierungseinstellung) nicht verändert werden und ist immer die letzte Regel, die abgearbeitet wird. Diese Regel blockt allen nicht explizit erlaubten Verkehr von irgendwo nach irgendwo. Die Existenz dieser Regel bedeutet auch, dass direkt nach der Installation des ISA Server 2004 "nichts funktioniert". Obwohl das auch schon beim ISA Server 2000 so der Fall war, verwirrt das immer noch viele Administratoren. In der Vergangenheit war es bei Microsoft Produkten (leider) fast immer so, dass nach einer weiter-weiter-weiter-fertig Installation alles aktiviert war und das Produkt sofort benutzt werden konnte. Beim ISA ist das (verständlicherweise) anders. Hier muss im

zweiten Schritt alles konfiguriert werden, was erlaubt werden soll. Der Grund liegt auf der Hand: erstens handelt es sich um eine Firewalllösung und zweitens wurde der ISA Server nach dem Microsoft-Grundsatz von Trustworthy Computing entwickelt. Dies sieht man übrigens auch in der Stabilität des Produktes. Vier Jahre nach Verfügbarkeit des ISA Server 2000 gibt es gerade mal ein Dutzend Hotfixe und Servicepacks. Schwerwiegende Sicherheitslücken waren nicht darunter. Auch wurde es bislang nicht geschafft, einen ordentlich konfigurierten ISA Server zu "hacken" (was auch immer man unter "hacken" verstehen möchte).

Erstellen und verwenden von Zeitplänen

Die Informationen in diesem Artikel beziehen sich auf:

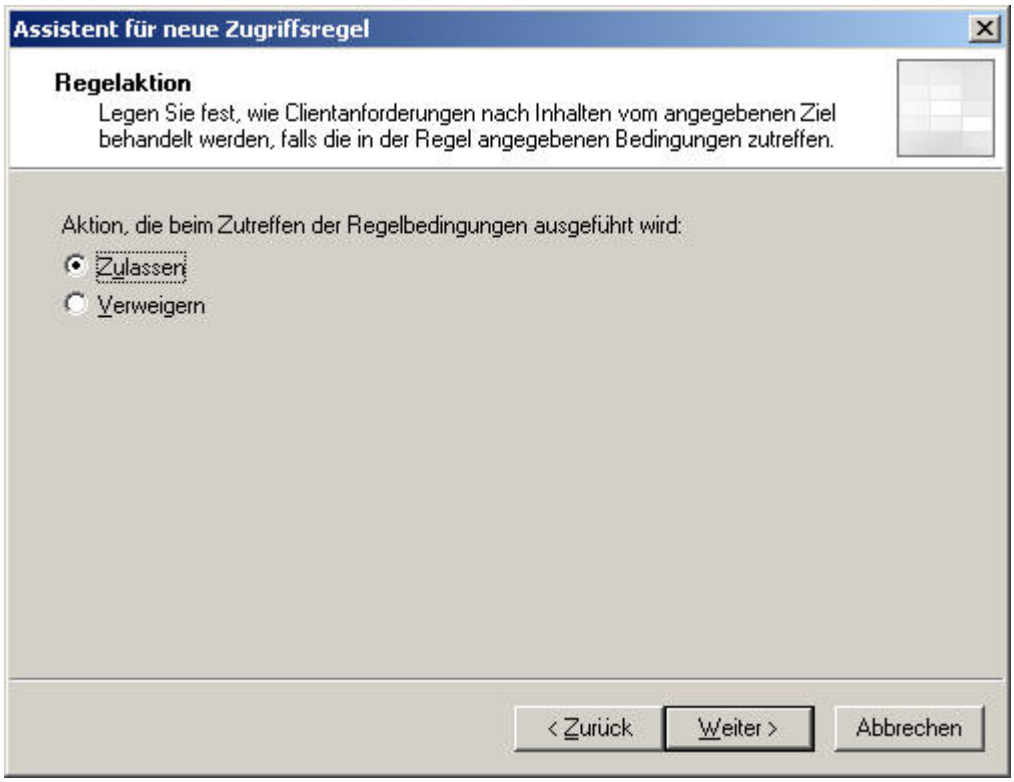
- Microsoft ISA Server 2004

Die Gültigkeit von Firewallrichtlinien kann unter anderem zeitgesteuert festgelegt werden. Damit ist es zum Beispiel möglich, internen Benutzern ohne Authentifizierung das Besuchen von Websites nur werktags zwischen 09:00 und 12:00 und von 14:00 bis 18:00 Uhr zu erlauben.

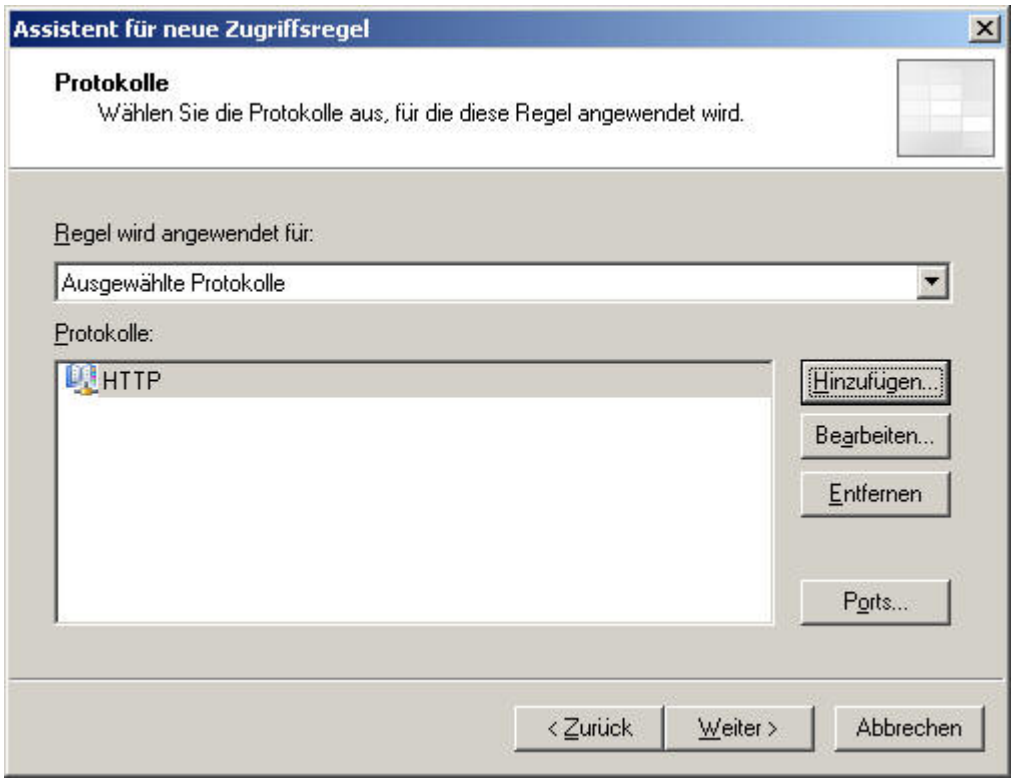
Der folgende Artikel beschreibt die wesentliche Schritte, um obiges Beispiel umzusetzen.

Dazu wird eine neue Firewallrichtlinie erstellt. Weitergehende Informationen über das Erstellen von Firewallrichtlinien können in diesem Artikel nachgelesen werden.

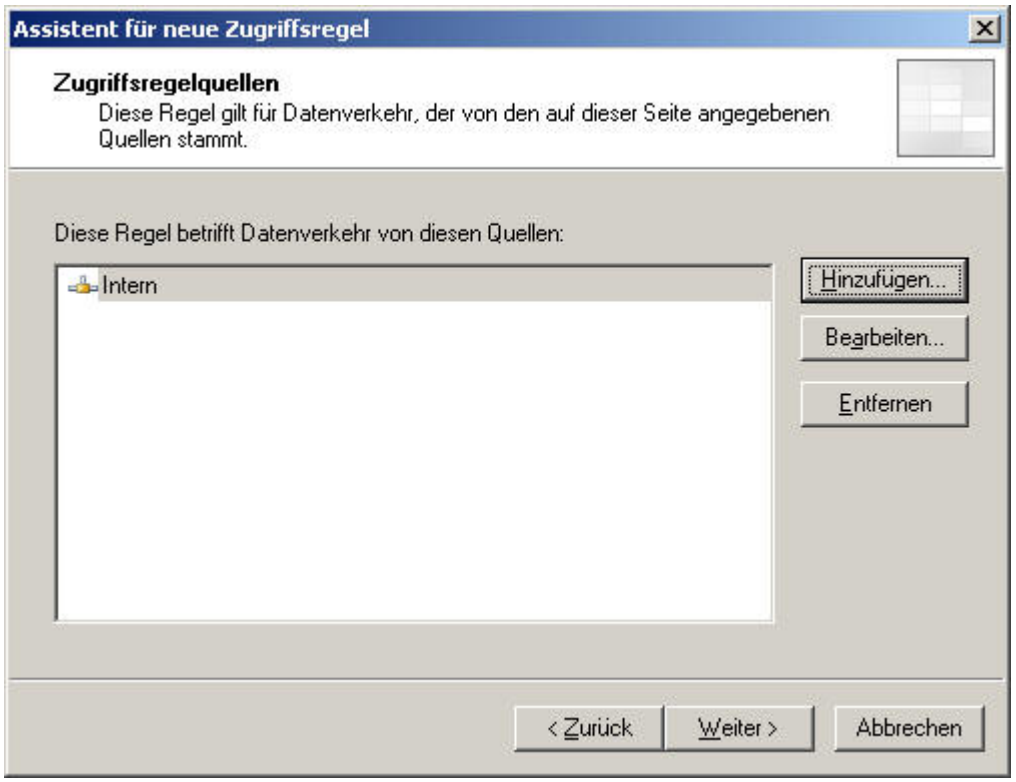
Hier sollte wie immer ein beschreibender Name verwendet werden.



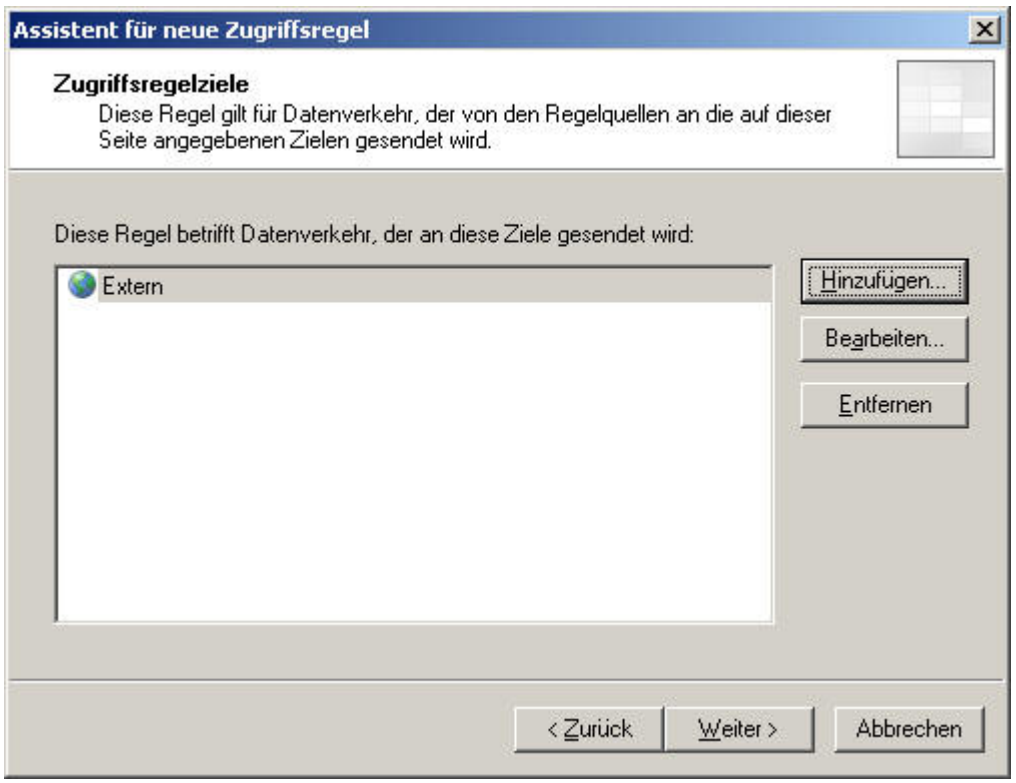
Diese Regel soll eine Zulassungsregel sein.



Die Regel gilt nur für das HTTP-Protokoll.



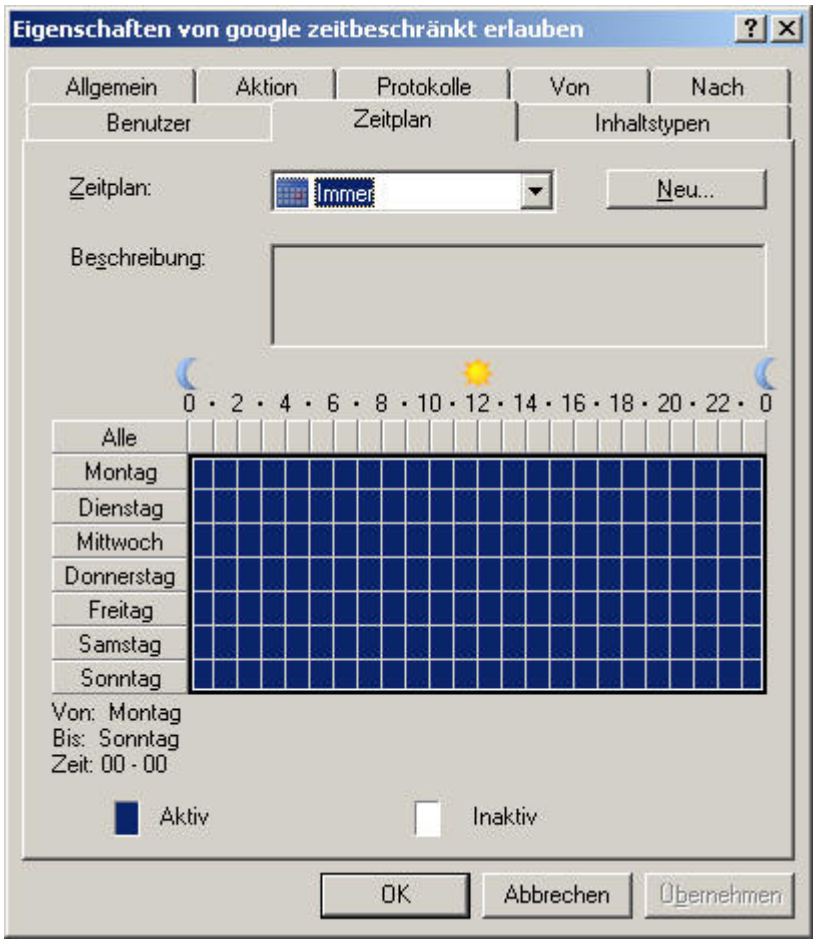
Da diese Regel alle Benutzer aus dem internen Netzwerk betrifft, wird das Netzwerk "Intern" als Quelle hinzugefügt.



In diesem Beispiel wird keine Einschränkung der erlaubten Websites festgelegt; daher wird das Netzwerk "Extern" als Ziel hinzugefügt.

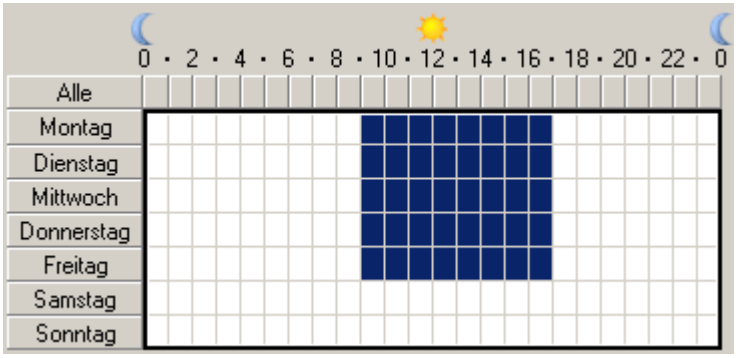
Im folgenden Dialog soll die Voreinstellung "Alle Benutzer" bestätigt werden. Danach kommt eine Zusammenfassung des Assistenten, welche z.B. für Dokumentationszwecke kopiert werden kann.

Die neue Firewallrichtlinie wurde somit erstellt. Nun muss noch der Zeitraum konfiguriert werden. Durch Doppelklick auf die Regel gelangt man zur Registerkarte "Zeitplan":

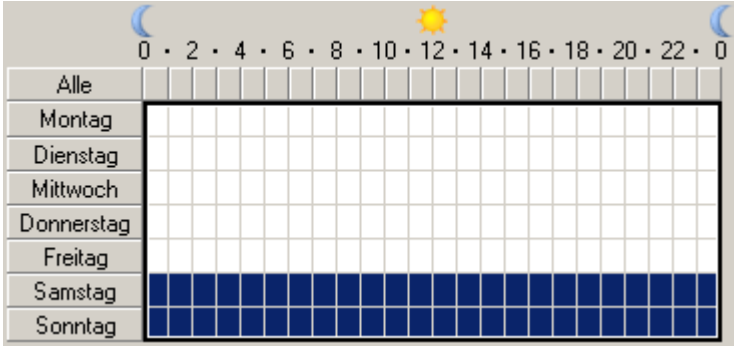


Die Standardeinstellung erlaubt die Regel zu jeder Zeit. Es gibt zwei vordefinierte Zeitpläne:

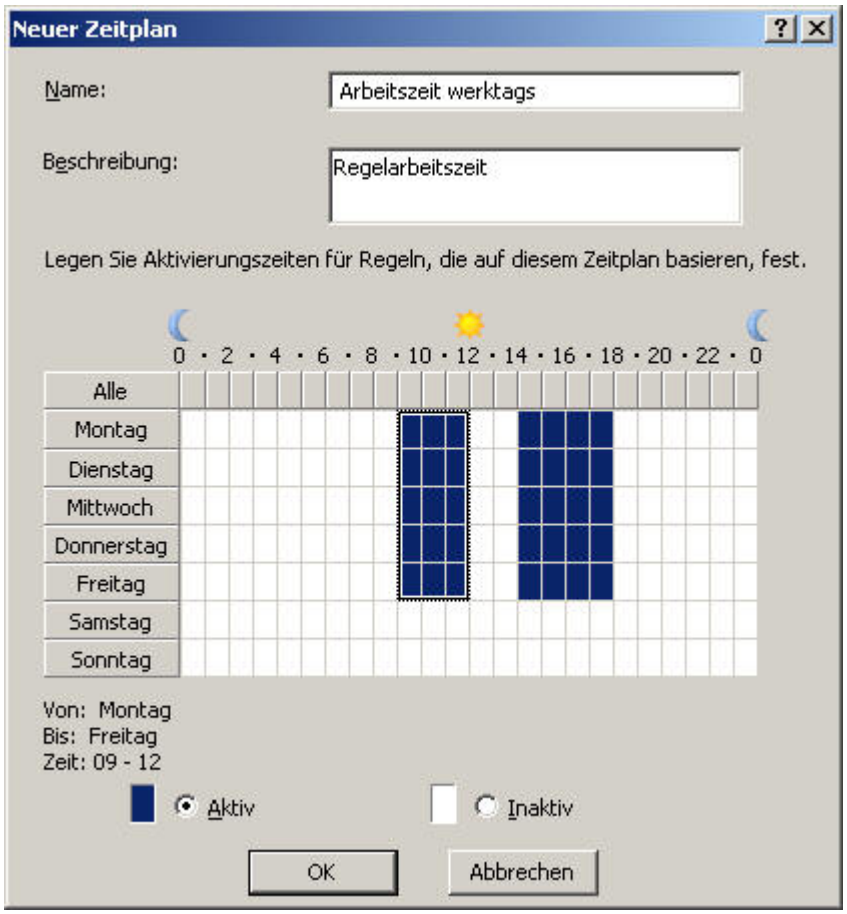
- Normale Arbeitszeit



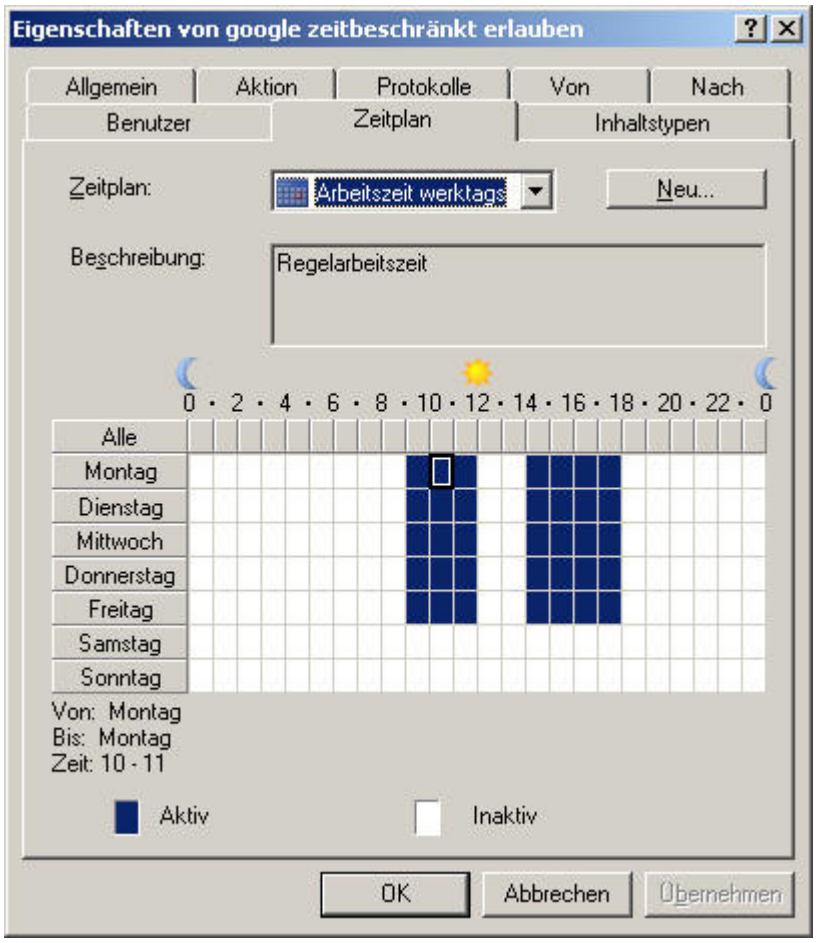
- Wochenende



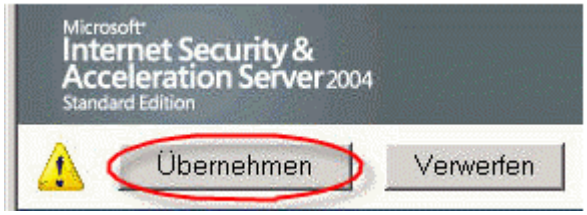
Durch klicken auf "Neu" kann ein neuer Zeitplan definiert werden. Für das obige Beispiel wird ein neuer Zeitplan benötigt.



Anschließend wird der neu erstellte Zeitplan ausgewählt:



Damit die Regel aktiv wird, muss die Konfigurationsänderung übernommen werden:



ISA Server Clients - Teil 1: Der SecureNAT-Client

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Das Kapitel über die vom ISA Server unterstützen Clients teilt sich in drei Artikel auf:

- Teil 1: Der SecureNAT-Client
- Teil 2: Der Firewallclient
- Teil 3: Der Webproxyclient

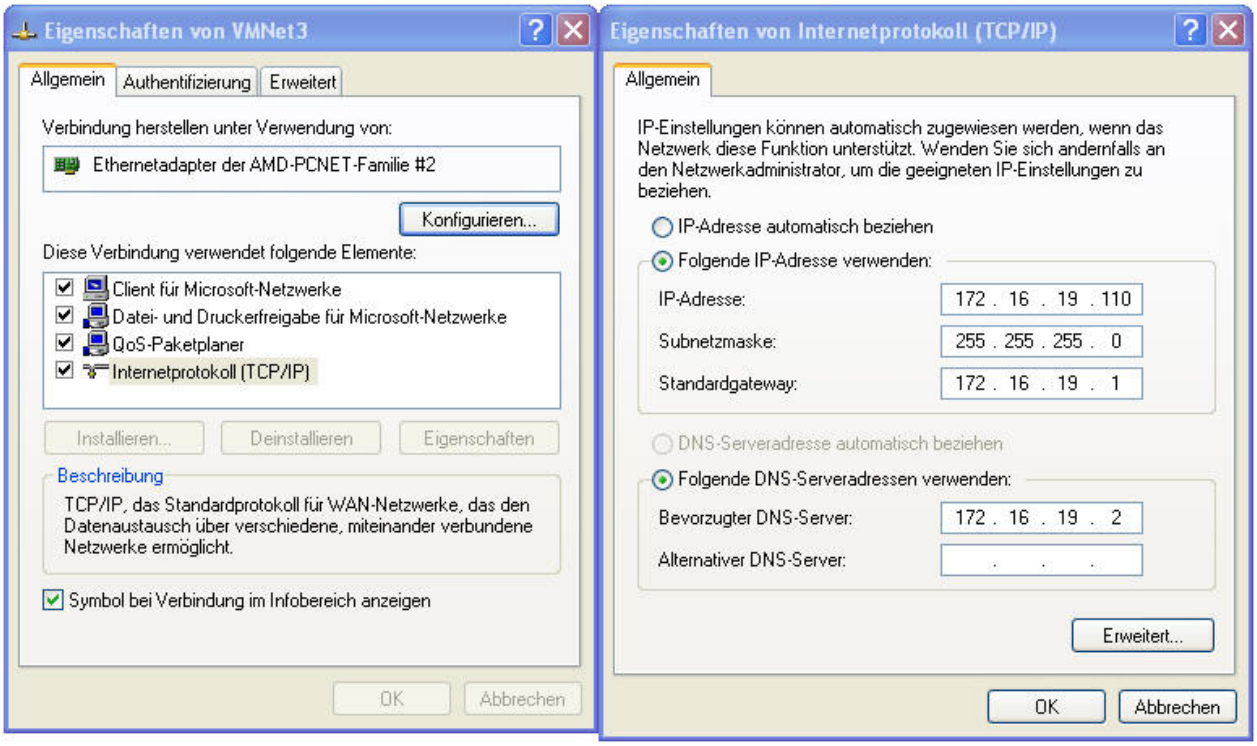
Der SecureNAT-Client

Ein SecureNAT-Client ist ein Computer, auf dem keine Firewallclientsoftware installiert ist. SecureNAT-Clients können von den meisten Funktionen ISA Server profitieren. Dies schließt die meisten Zugriffssteuerungsfunktionen ein, mit Ausnahme der Unterstützung von komplexen Protokollen (sofern kein Anwendungsfilter dafür vorhanden ist) und Authentifizierung auf Benutzerebene.

Obwohl SecureNAT-Clients keine spezielle Software benötigen, muss das Standardgateway so konfigurieren werden, dass der gesamte für das Internet bestimmte Datenverkehr über ISA Server (direkt oder indirekt) durch einen Router gesendet wird. Dies kann entweder manuell oder durch einen DHCP-Server vorgegeben werden.

Manuelle Konfiguration eines Clients zum SecureNAT-Client:

In den Eigenschaften der Netzwerkverbindung des Clients (in der Regel ist nur eine mit dem Namen "LAN-Verbindung" vorhanden) die Eigenschaften von "Internetprotokoll (TCP/IP)" aufrufen:

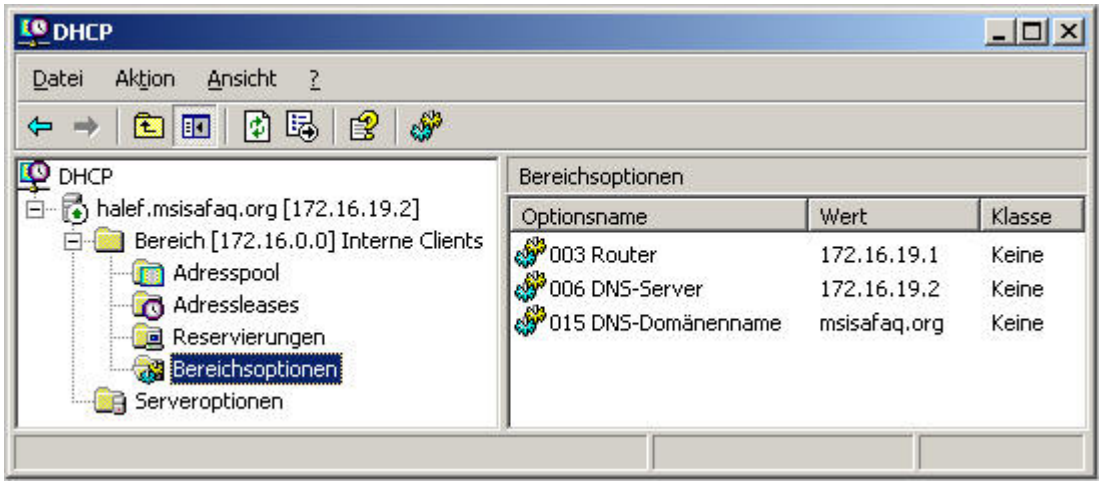


Im Beispiel für diesen Artikel hat der ISA Server die IP-Adresse 172.16.19.1, der interne DC mit DNS die Adresse 172.16.19.2

Konfiguration über DHCP-Server:

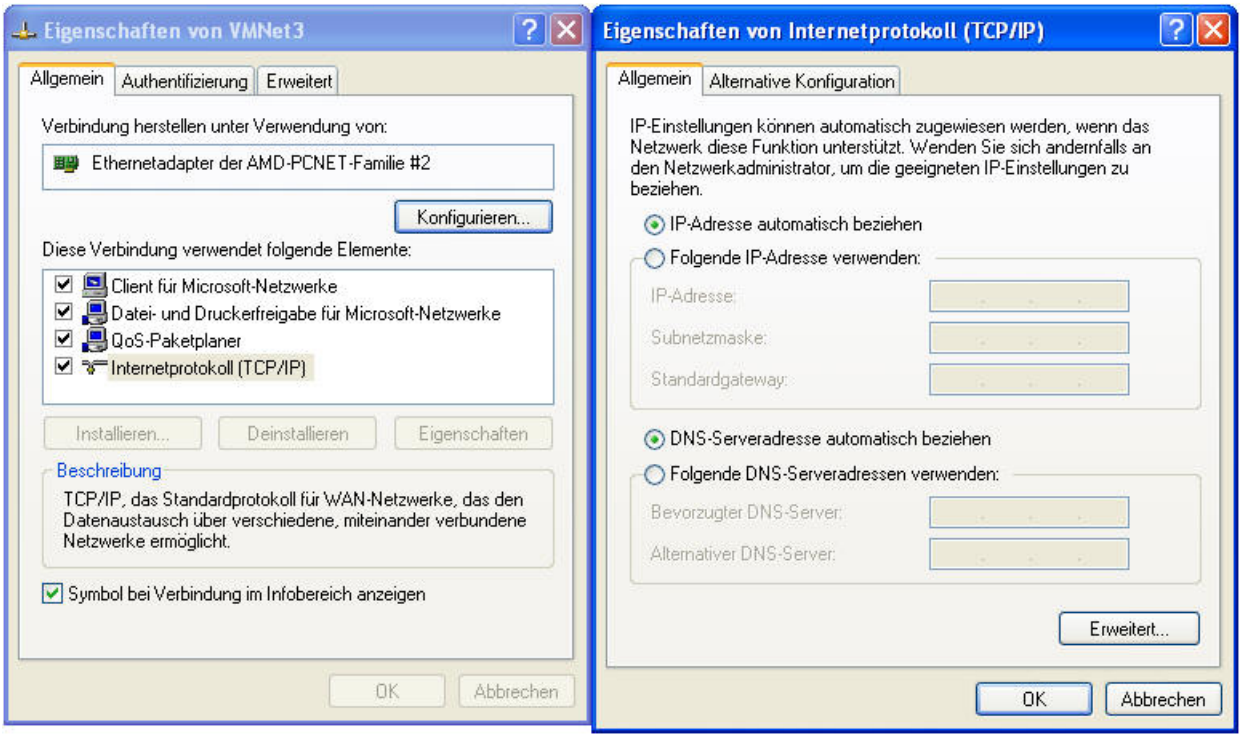
Grundsätzliche Informationen zur Verwendung eines DHCP-Servers können u.a. in der Online-Hilfe des Windows Servers nachgelesen werden.

Die Information zum Standardgateway werden in der DHCP-Option "003 Router" hinterlegt, die entweder über Bereichs- oder über Serveroptionen hinzugefügt wird:



Im oberen Beispiel werden den Clients auch Informationen zu DNS mitgegeben.

In den Eigenschaften der Netzwerkverbindung des Clients (in der Regel ist nur eine mit dem Namen "LAN-Verbindung" vorhanden) die Eigenschaften von "Internetprotokoll (TCP/IP)" aufrufen:



Die Registerkarte "Alternative Konfiguration" ist nur bei automatischer IP-Einstellung verfügbar. Hier kann für den Fall, dass kein DHCP-Server verfügbar ist eine feste IP-Adresse konfiguriert werden. Diese Funktion ist erst ab Windows XP verfügbar.

Anfragen von SecureNAT-Clients werden vom Firewalldienst verarbeitet. Dabei ist keine Authentifizierung auf Benutzerbasis möglich, es können nur Regeln anhand von IP-Adressen erstellt werden.

SecureNat-Clients werden im reinen Cachemodus nicht unterstützt.

SecureNAT-Clients benötigen immer eine Firewallrichtlinie für ausgehenden Verkehr. Selbst wenn eine Protokollregel vorhanden ist, die den gesamten IP-Datenverkehr frei gibt betrifft das nur die Protokolle/Ports, für die eine Protokolldefinition vorhanden ist.

Ein SecureNAT-Client muss sich selber um die DNS-Auflösung kümmern. Beim Webproxy- und/oder Firewallclient ist der ISA Server für die Namensauflösung zuständig.

ISA Server Clients - Teil 2: Der Firewall Client

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Das Kapitel über die vom ISA Server unterstützen Clients teilt sich in drei Artikel auf:

- Teil 1: Der SecureNAT-Client
- Teil 2: Der Firewallclient
- Teil 3: Der Webproxyclient

Einleitung

Dieser Artikel beschreibt die Funktionsweise des Microsoft ISA Server 2004 Firewall Client und dessen Konfiguration.

Ein Firewallclient im Microsoft Jargon ist ein Computer, auf dem die Firewallclientsoftware installiert und aktiviert ist. Auf dem Firewallclientcomputer wird eine Winsock-Anwendung ausgeführt, die den Microsoft-Firewalldienst von ISA Server 2004 verwendet.

Wie funktioniert der Firewall Client

Beim Installieren eines Firewallclients auf dem Clientcomputer werden nicht die einzelnen Winsock-Anwendungen konfiguriert. Stattdessen wird ein gemeinsames Winsock genutzt, der auch von den anderen Anwendungen verwendet wird. Der Firewallclient fängt anschließend die Aufrufe der Anwendungen ab und ermittelt, ob die Anforderung an den ISA Server-Computer weitergeleitet wird.

Sie können festlegen, ob für das jeweilige Netzwerk (welches Sie am ISA Server konfiguriert haben) die Firewallclientunterstützung aktiviert werden soll. Bei aktivierter Firewallclientunterstützung nimmt der ISA Server 2004 eingehende Anforderungen an Port 1745 entgegen. Wenn ein Firewallclient über eine Winsock-Anwendung ein Objekt von einem Computer anfordert, überprüft der Client, ob der betreffende Computer als lokaler Computer eingestuft ist. Eine Adresse gilt als lokal, wenn sie im Adressbereich des jeweiligen Netzwerks enthalten ist.

Ist der anzurufende Server/Computer nicht lokal, wird die Anforderung an den Firewalldienst gesendet. Der Firewalldienst verarbeitet die Anforderung und leitet diese (basierend auf den Firewallrichtlinien) an das entsprechende Ziel weiter. Die Firewallclientsoftware kann, ebenfalls wie der Webproxy Client (allerdings nur für HTTP/HTTPS/FTP), Windows-Benutzerinformationen, die für Authentifizierungszwecke benötigt werden, an den ISA Server-Computer senden. Der FW-Client ist der einzige Client, welcher eine

Benutzerauthentifizierung für jedes Protokoll unterstützt und ohne einen Anwendungsfilter komplexe Protokolle und sekundäre Verbindungen unterstützt.

Für eine wesentlich technischere Übersicht über den ISA Server Firewall Client, lesen Sie folgenden Artikel.

Was ist Winsock

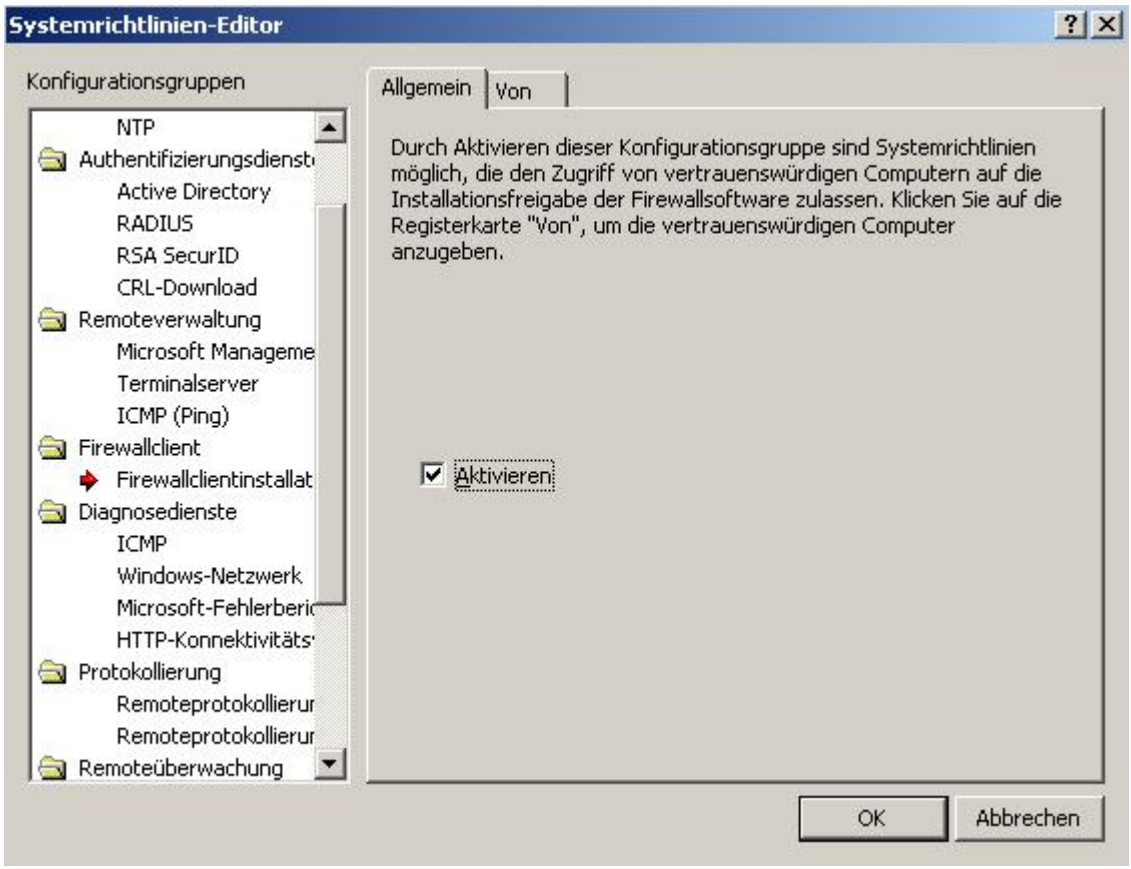
Winsock ist die Kurzform für Windows Socket. Dabei handelt es sich um eine API (Application Programming Interface), die Windows-Programmen über das TCP/IP-Netzwerkprotokoll die Kommunikation mit anderen Computern ermöglicht.

Allgemeines

Die ISA Server-Clientinstallationsdateien befinden sich normalerweise in einem Ordner auf dem ISA Server-Computer mit dem Freigabenamen **ISA_Servername/MSPClnt**. Das muss seit ISA Server 2004 aber nicht mehr sein. Sie können die FW-Client Installationsfreigabe auch auf einem anderen Server zur Verfügung stellen.
Die Firewallclientsoftware darf **nicht** auf dem ISA Server-Computer installiert werden.
Bei der Installation wird die Firewallclientanwendung aktiviert.
Die Firewallclientsoftware kann auf Clientcomputern unter folgenden Betriebssystemen installiert werden:

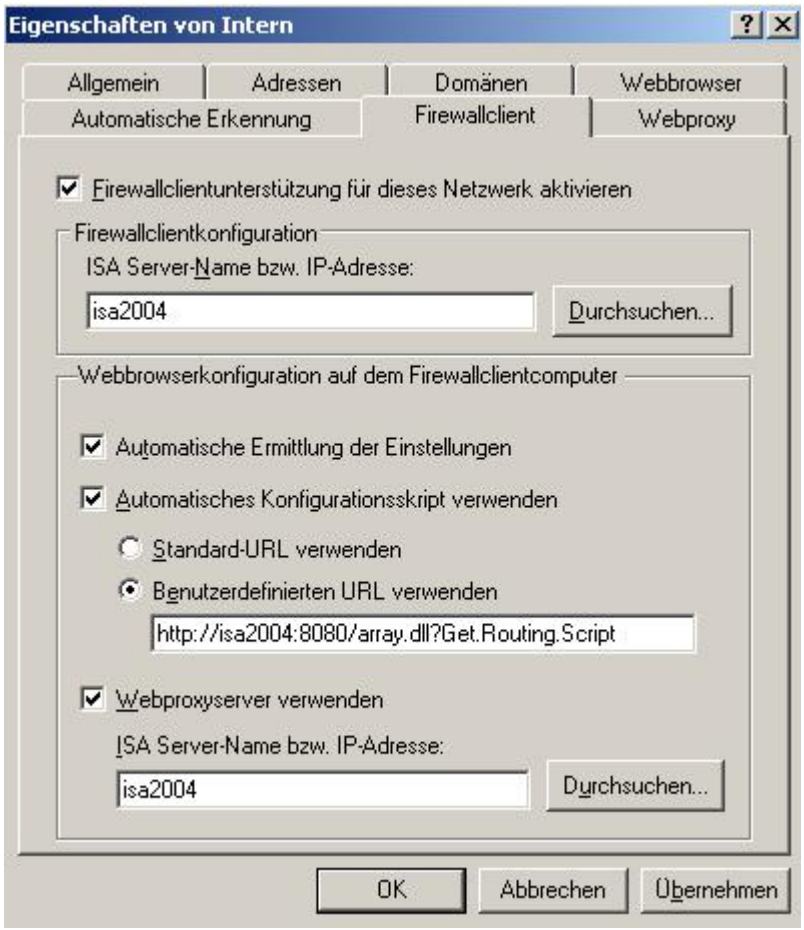
- Microsoft Windows Server 2003
- Windows 2000 Server
- Windows XP
- Windows Millennium Edition
- Windows NT 4.0.
- Windows 98 SE (wenn IE ab Version 5 installiert ist)

Clientcomputer können auf die Firewallclientfreigabe zugreifen, wenn die Systemrichtlinien-Konfiguration **Firewallclient** - **Firewallclientinstallation** für Firewallclient aktiviert ist.
Diese Konfiguration wird standardmäßig bei der Installation der Firewallclientfreigabe aktiviert.



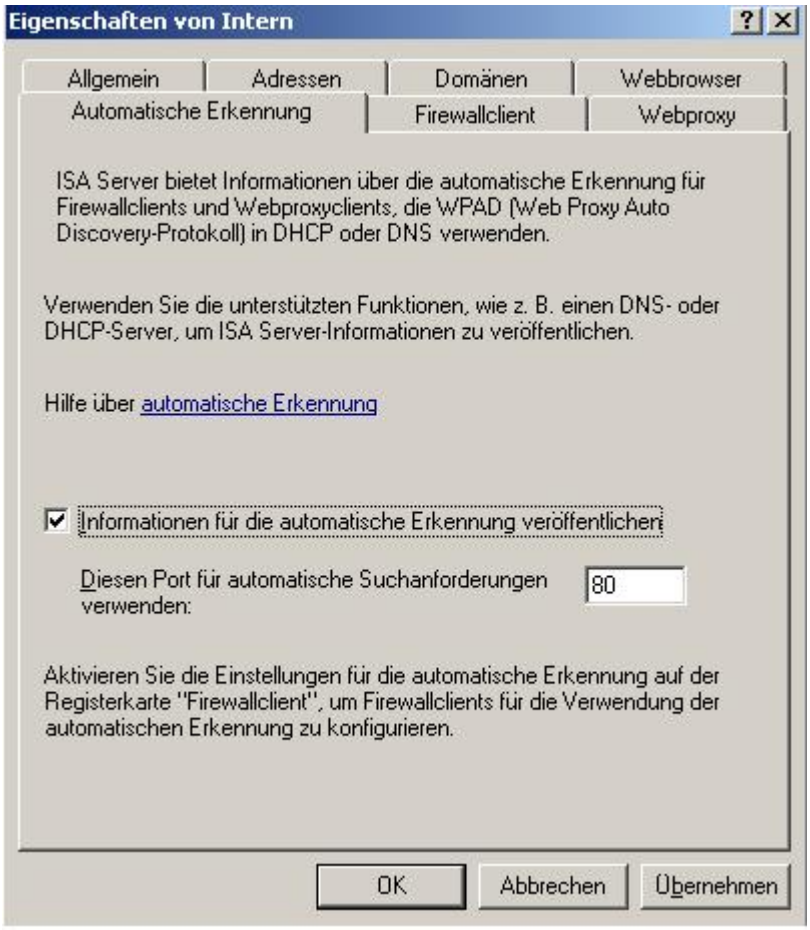
Aktivierung des Servers für die Firewall Client Verwendung

Starten Sie die ISA Server Verwaltungskonsole, navigieren Sie zu **Konfiguration** - **Netzwerke** - und dann in die Eigenschaften des Netzwerkobjektes **Intern** im Reiter **Netzwerke.** Klicken Sie dort den Reiter **Firewallclient** an und nehmen Sie die notwendigen Einstellungen vor.



Im Bereich **Webbrowserkonfiguration auf dem Firewallclientcomputer** können Sie ein **automatisches Konfigurationsskript** angeben. Hier ist die Angabe einer .INS Datei des IEAK (Internet Explorer Administration Kit) möglich, mit welchem weitere Einstellungen konfiguriert werden. Lesen Sie hier mehr zum IEAK.

Der ISA Server kann für die automatische Erkennung des ISA Servers für den Firewall- und Webproxy Client konfiguriert werden.



Für weitere Informationen rund um das Thema **Automatische Erkennung**, lesen Sie folgenden Artikel.

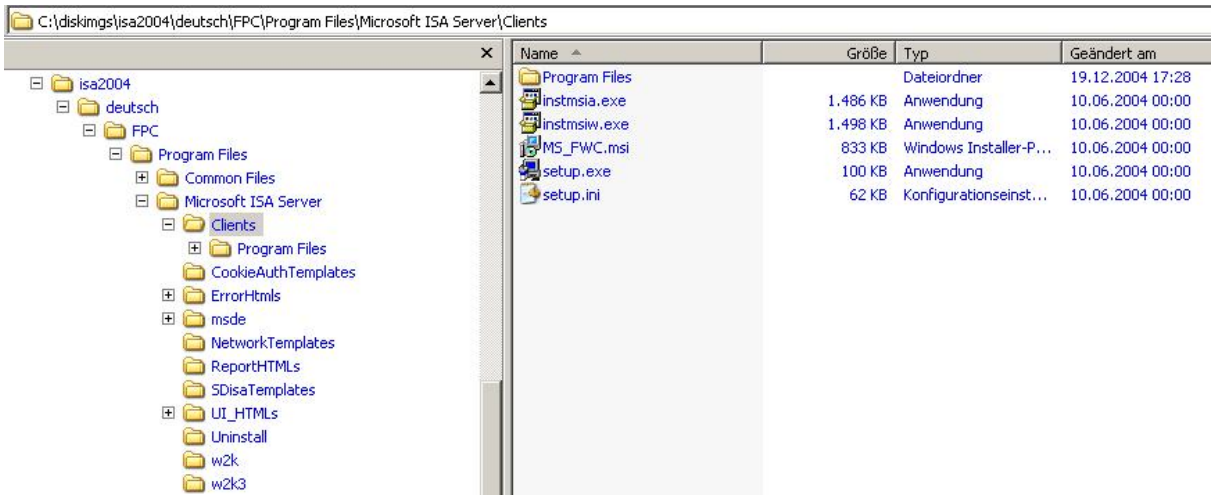
Firewall Client Installation

Der Firewall Client kann auf verschiedenen Arten installiert werden:

- Händische Installation
- Installation über die Softwareverteilungsfunktion der Gruppenrichtlinien von Windows 2000 / 2003
- Unbeaufsichtigte Installation über ein Skript

Händische Installation

Die händische Installation erfolgt durch manuelles Ausführen der FWC (Firewall Client) Setup-Routine (`SETUP.EXE`).



Folgen Sie den Anweisungen des Setup Wizards.

Der Firewall Client ist schnell installiert.

Angabe, ob der ISA Computer händisch eingetragen werden soll oder ob der ISA ´Server Computer automatisch ermittelt werden soll. Für die automatische Ermittlung sind zusätzliche Schritte erforderlich.

Installation über die Softwareverteilungsfunktion der Gruppenrichtlinien von Windows 2000 / 2003

Sie können den Firewall Client problemlos über die Softwareverteilungsfunktion der Gruppenrichtlinien von Windows 2000/2003 verteilen. Microsoft liefert für die Installation ein passendes MSI File mit. Kopieren Sie das Verzeichnis Clients von der ISA CD in die Softwareverteilungsfreigabe. Für eine detaillierte Beschreibung der Softwareverteilung, lesen Sie den Artikel **Softwarezuweisung** unter **HowTo** auf der folgenden Webseite.

Unbeaufsichtigte Installation über ein Skript

So führen Sie eine unbeaufsichtigte Firewallclientinstallation durch:
Geben Sie an der Eingabeaufforderung auf dem Firewallclientcomputer folgendes ein:

Pfad\Setup /v"[SERVER_NAME_OR_IP=ISA_Servername] [ENABLE_AUTO_DETECT={1|0}] [REFRESH_WEB_PROXY={1|0}] /qn"

Erklärung:

Pfad steht für den Pfad zu den freigegebenen ISA Server-Clientinstallationsdateien. Diese Dateien befinden sich normalerweise auf dem ISA Server-Computer in einem Ordner mit dem Freigabenamen ISA\MSPclnt.
ISA_Servername steht für den Namen des ISA Server-Computers, zu dem der Firewallclient eine Verbindung herstellen soll.
Der Parameter **ENABLE_AUTO_DETECT=1** gibt an, dass der Firewallclient automatisch den ISA Server-Computer erkennt, über den Verbindungen hergestellt werden ist.
Der Parameter **REFRESH_WEB_PROXY=1** gibt an, dass die Firewallclientkonfiguration mit der Webproxykonfiguration aktualisiert werden soll, die auf dem ISA Server-Computer definiert wurde.

Unbeaufsichtigte Deinstallation

Um eine unbeaufsichtigte Deinstallation durchzuführen, geben Sie an einer Eingabeaufforderung folgendes ein:

MsiExec.exe /X {199B7F78-69B7-47C5-8D4B-A3ED1391FB6B} /qn

Um dieses Verfahren durchführen zu können, müssen Sie auf dem Clientcomputer Mitglied der Gruppe Administratoren sein.

Erweiterte Firewallclienteinstellungen

Nach der Installation übernimmt die Firewallclientsoftware die Einstellungen, die durch den ISA Server 2004-Computer konfiguriert wurden, von dem aus die Firewallclientanwendung installiert wurde. Durch diese Servereinstellungen werden unter anderem die **automatische Webproxykonfiguration**, der **ISA Server-Name**, die **automatische Erkennung von ISA Server** sowie andere Funktionen bestimmt.

Nachdem die Firewallclientsoftware installiert ist, aktualisiert der ISA Server 2004 diese Clienteinstellungen bei jedem Neustart eines Clientcomputers und alle sechs Stunden nach der ersten Aktualisierung.

Zusätzlich zu diesen Einstellungen aktualisiert ISA Server den FW-Client regelmäßig mit Informationen zu IP-Adressen, die der Client als lokale Adressen erkennen soll.

Für die meisten Winsock-Anwendungen funktioniert die Standardfirewall-Clientkonfiguration ohne jegliche zusätzliche Änderungen. In einigen Fällen müssen Sie jedoch Clientkonfigurationsinformationen hinzufügen (ein Beispiel hierfür ist Outlook). Der Firewallclient kann für jeden Benutzer und für jeden Computer lokal auf dem Firewallclientcomputer konfiguriert werden. Die Konfiguration erfolgt, indem Änderungen an den INI-Dateien vorgenommen werden, die auf dem Firewallclientcomputer installiert sind.

Sie können die Standardeinstellungen für alle Komponenten nach der Installation ändern. Die neuen Konfigurationseinstellungen werden erst beim Aktualisieren der Clientkonfiguration wirksam.

INI-Dateien

Die Konfigurationsdaten werden in mehreren Dateien gespeichert, die auf dem Firewallclientcomputer installiert sind. Bei der Installation des Firewallclients auf dem Computer werden im einzelnen folgende Dateien auf dem Firewallclientcomputer installiert:

- Common.ini
- Management.ini
- Application.ini

Common.ini

In der Datei COMMON.INI werden allgemeine Konfigurationen für alle Anwendungen festgelegt.

Beispiel für den Inhalt dieser Datei

[Common]
ServerName=ISA2004 (gibt den ISA Server 2004 Computernamen an)
Disable=0 (gibt an, ob der ISA FW Client deaktiviert ist)
Autodetection=0 (gibt an, ob eine automatische Firewallerkennung aktiv ist)

Management.ini

Die Datei Management.ini werden die Konfigurationseinstellungen für die Firewallclientverwaltung festgelegt.

Beispiel für den Inhalt dieser Datei

[TrayIcon]
TrayIconVisualState=1 (gibt an, ob das ISA FW Client Symbol in der Taskleiste auftauchen soll)

Application.ini

Die Datei Application.ini enthält Konfigurationseinstellungen für bestimmte Anwendungen.

Beispiel für den Inhalt dieser Datei

[FW_Client_Proggi]
Disable=0
NameResolution=R
LocalBindTcpPorts=4711
LocalBindUdpPorts=4711-4723, 7400-7460
RemoteBindTcpPorts=32
RemoteBindUdpPorts=3200-3250
ServerBindTcpPorts=200-400
ProxyBindIp=80:192.168.1.23
Persistent=1
ForceCredentials=1
NameResolutionForLocalHost=L

Diese Dateien werden auf Betriebssystemebene für alle am Computer angemeldeten Benutzer erstellt und können für jeden einzelnen Benutzer auf dem Computer erstellt werden. Die Einstellungen für einzelne Benutzer haben Vorrang gegenüber den allgemeinen Konfigurationseinstellungen. Diese Dateien werden abhängig vom Betriebssystem an verschiedenen Speicherorten erstellt. Bei Windows XP werden die Dateien in zwei Ordner kopiert:

\Dokumente und Einstellungen\All Users\\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004
\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004

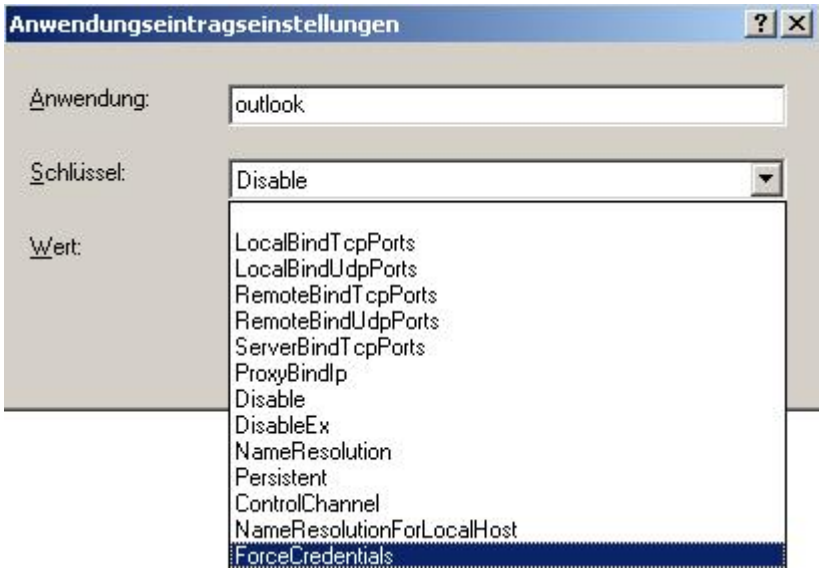
Einstellungen in der Datei Application.ini können auch zentral am ISA Server vorgenommen werden und gelten dann für alle FW-Clients.

Starten Sie dazu die ISA Server Verwaltungskonsole und navigieren Sie zu **Konfiguration** - **Allgemein** - **Firewallclienteinstellungen definieren** und dann in den Reiter **Anwendungseinstellungen.**

Beispiel Outlook

In der deutschen ISA Newsgroup gibt es häufiger Aússagen, dass Outlook bei aktiviertem Firewall Client nicht richtig funktioniert. Schuld ist hier die Standard Einstellung des ISA Servers für den FW Client, Outlook für die Verwendung über die Firewall zu deaktivieren. Die Anwendung **outlook** hat per Default einen Schlüssel **Disable** dessen Wert auf **1** gesetzt ist. Damit Outlook über den ISA Server funktioniert, setzen Sie den Wert auf **0**.

Weitere Anwendungseintragseinstellungen sind:



Beschreibung der Einstellungen (aufbereitet aus der ISA Server Onlinehilfe)

Eintrag	Beschreibung
ServerName	Gibt den Namen des ISA Server-Computers an, zu dem der Firewallclient eine Verbindung herstellen soll
Disable	Mögliche Werte: 0 oder 1. Ist der Wert auf 1 eingestellt, wird die Firewallclientanwendung für die betreffende Clientanwendung deaktiviert
DisableEx	Werte: 0 oder 1. Ist der Wert auf 1 eingestellt, wird die Firewallclientanwendung für die betreffende Clientanwendung deaktiviert. Dies betrifft ausschließlich den Firewallclient für ISA Server 2004. Wenn diese Option aktiviert ist, wird die Einstellung Disable außer Kraft gesetzt
NameResolution	Mögliche Werte: "L" oder "R". Standardmäßig werden Domänennamen in dezimaler, durch Punkte getrennter Schreibweise bzw. Internetdomänennamen zur Namensauflösung an den ISA Server-Computer umgeleitet. Alle anderen Namen werden auf dem lokalen Computer aufgelöst. Ist dieser Wert auf "R" eingestellt, werden alle Namen zur Auflösung an den ISA Server-Computer umgeleitet ("Redirection"). Ist dieser Wert auf L eingestellt, werden alle Namen auf dem lokalen Computer aufgelöst ("Local")
LocalBindTcpPorts	Gibt einen TCP-Port (Transmission Control Protocol), eine TCP-Liste oder einen TCP-Bereich mit lokaler Bindung an
LocalBindUdpPorts	Gibt einen UDP-Port (User Datagram Protocol), eine UDP-Liste oder einen UDP-Bereich mit lokaler Bindung an
RemoteBindTcpPorts	Gibt einen TCP-Port, eine TCP-Liste oder einen TCP-Bereich mit Remotebindung an
RemoteBindUdpPorts	Gibt einen UDP-Port, eine UDP--Liste oder einen UDP-Bereich mit Remotebindung an
ServerBindTcpPorts	Gibt einen TCP-Port, eine TCP-Liste oder einen TCP-Bereich für alle Ports an, die mehr als eine Verbindung annehmen sollen
Persistent	Mögliche Werte: 0 oder 1. Ist dieser Wert auf 1 eingestellt, kann ein bestimmter Serverstatus auf dem ISA Server-Computer aufrecht erhalten werden, wenn ein Dienst beendet und neu gestartet wird und der Server nicht antwortet. Der Client sendet während einer aktiven Sitzung regelmäßig eine Keep-Alive-Meldung an den Server. Antwortet der Server nicht, versucht der Client beim Neustart des Servers, den Status der gebundenen und abhörenden Sockets wieder herzustellen
ForceCredentials	(Kann nur am Firewallclientcomputer eingestellt werden.) Wird verwendet, wenn ein Windows-Dienst oder eine Windows-Serveranwendung als Firewallclientanwendung ausgeführt wird. Ist dieser Wert auf 1 eingestellt, wird die Verwendung anderer Anmeldeinformationen für die Benutzerauthentifizierung erzwungen. Diese Informationen sind lokal auf dem Computer gespeichert, auf dem der Dienst ausgeführt wird. Die Benutzeranmeldeinformationen werden auf dem Clientcomputer mit der Anwendung Credtool.exe gespeichert, die zum Lieferumfang der Firewallclientsoftware gehört. Die Benutzeranmeldeinformationen

	müssen auf ein Benutzerkonto verweisen, das von ISA Server authentifiziert werden kann. Dieses Konto kann sich auf dem ISA Server-Computer oder einer für ISA Server vertrauenswürdigen Domäne befinden. Das Benutzerkonto ist normalerweise so eingestellt, dass es nicht abläuft. Andernfalls müssen die Benutzerinformationen jeweils vor Ablauf des Kontos erneuert werden
NameResolution ForLocalHost	Mögliche Werte sind "L" (Standardeinstellung), "P" oder "E". Gibt an, wie der lokale Computername (Client) beim Aufruf der API gethostbyname aufgelöst wird. Der Computername LocalHost wird durch Aufruf der Winsock-API-Funktion gethostbyname() unter Verwendung der Zeichenfolge LocalHost, einer leeren Zeichenfolge oder eines NULL-Zeichenfolgenzeigers aufgelöst. Winsock-Anwendungen rufen gethostbyname(LocalHost) auf, um ihre lokale IP-Adresse zu suchen und an einen Internetserver zu senden. Ist die Option auf "L" eingestellt, gibt gethostbyname() die IP-Adressen des lokalen Hostcomputers zurück. Ist die Option auf "P" eingestellt, gibt gethostbyname() die IP-Adressen des ISA Server-Computers zurück. Ist die Option auf "E" eingestellt, gibt gethostbyname() nur die externen IP-Adressen des ISA Server-Computers zurück – die IP-Adressen, die sich nicht in der lokalen Adresstabelle befinden
ControlChannel	Mögliche Werte: "Wsp.udp" oder "Wsp.tcp" (Standardeinstellung). Gibt den Wert des verwendeten Steuerkanals an
EnableRouteMode	Mögliche Werte sind 0 und 1 (Standardeinstellung). Wenn EnableRouteMode auf 1 eingestellt und ein Routeverhältnis zwischen dem Firewallclientcomputer und dem angeforderten Ziel eingerichtet ist, wird die IP-Adresse des Firewallclients als Quelladresse verwendet. Ist dieser Wert auf 0 eingestellt, wird die IP-Adresse des ISA Server-Computers verwendet. Dieses Flag wird von älteren Versionen des Firewallclients nicht unterstützt

Reihenfolge der Anwendung der Einstellungen

Die INI-Dateien im Ordner des Benutzers haben Vorrang.
Als Nächstes überprüft der Firewallclient den Inhalt des Ordners All Users. Alle weiteren Konfigurationseinstellungen werden ggf. übernommen. Falls eine festgelegte Konfigurationseinstellung zu den entsprechenden benutzerspezifischen Einstellungen im Widerspruch steht, wird sie ignoriert.
Die Firewallclientanwendung erkennt den ISA Server-Computer, mit dem eine Verbindung hergestellt werden soll, entsprechend den in der Firewallclientverwaltung festgelegten Einstellungen.
Schließlich untersucht der Firewallclient die Einstellungen auf Serverebene. Alle für ISA Server festgelegten Konfigurationseinstellungen werden übernommen. Falls eine festgelegte Konfigurationseinstellung zu den entsprechenden benutzer- oder computerspezifischen Einstellungen im Widerspruch steht, wird sie ignoriert.

Lokale Adressen des Firewallclients

Standardmäßig betrachtet der Firewallclient alle Adressen im Netzwerk, für die dieser Client konfiguriert ist, sowie die in der lokalen Routingtabelle auf dem Firewallclientcomputer angegebenen Adressen als lokale Adressen. Wenn beispielsweise der Firewallclient eine Verbindung zum Netzwerkadapter für das interne Netzwerk herstellt, werden alle im internen Netzwerk konfigurierten IP-Adressen als lokal angesehen. Bei jedem Versuch einer Winsock-Anwendung auf dem betreffenden Client, eine Verbindung zu einer IP-Adresse herzustellen, wird anhand der Datei **Locallat.txt** bestimmt, ob es sich bei der IP-Adresse um eine Adresse im internen Netzwerk handelt. Falls die Adresse als lokale Adresse angesehen wird, kommt es zu einer direkten Verbindungsherstellung. Wenn die Adresse nicht als lokale Adresse gilt, wird die Verbindung über den Microsoft-Firewalldienst auf ISA Server hergestellt.

LAT - Da ist sie wieder (aber nur auf der Clientseite)

Eine lokale Version dieser Informationen kann ebenfalls erstellt werden. Sie können mit Notepad eine benutzerdefinierte Datei für die lokale Adresstabelle (LAT) eines Clients unter dem Namen **Locallat.txt** erstellen und im Ordner \Dokumente und Einstellungen\All Users\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004 auf dem Firewallclientcomputer speichern. Sie können weitere IP-Adressbereiche hinzufügen, die der Client als Bestandteil des lokalen Netzwerks erkennt. Der Client bestimmt anhand der eigenen **Routingtabelle**, der **serverspezifischen Einstellungen** und der Datei **Locallat.txt,** welche IP-Adressen zum lokalen Netzwerk gehören.

Beim Erstellen der Datei **Locallat.txt** geben Sie die IP-Adresspaare in die Datei ein. Jedes Adresspaar definiert entweder einen IP-Adressbereich oder eine einzelne IP-Adresse. Das folgende Beispiel zeigt eine Datei **Locallat.txt** mit zwei Einträgen. Der erste Eintrag ist ein IP-Adressbereich und der zweite eine einzelne IP-Adresse.

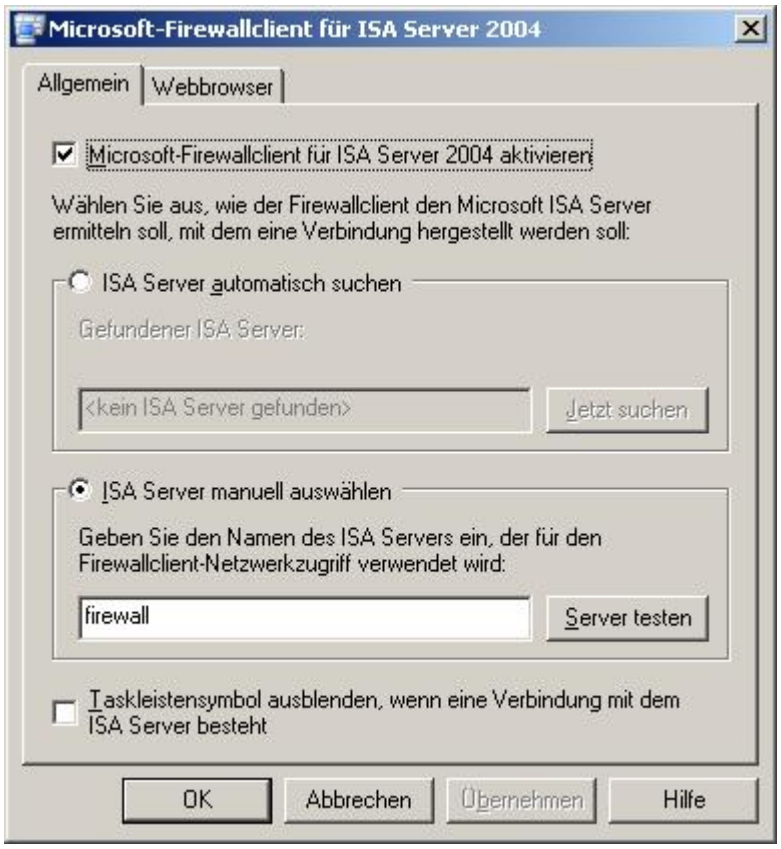
192.168.1.0 192.168.1.255 - gibt einen Netzwerkbereich an
192.168.1.18 192.168.1.18 - gibt eine IP-Adresse an.

Firewall Clienteinstellungen

Nach erfolgter Firewallclient-Installation, können Sie die Einstellungen des Firewall Clients modifizieren.

Klicken Sie dazu doppelt auf das ISA Icon im Tray.

Eine Übersicht über sämtliche FW-Clientkonfigurationseinstellungen finden Sie in der Datei C:\Programme\Microsoft Firewall Client 2004\ISAClient.htm



Wenn Sie verhindern wollen, dass Benutzer den Firewall Client deaktivieren, entfernen Sie sämtliche Benutzerberechtigungen auf die Datei COMMON.INI und geben Sie dem Benutzer statt dessen nur Leseberechtigungen auf die Datei, damit der Benutzer die Konfiguration lesen kann (System und Administratoren sollten natürlich weiterhin Vollzugriff haben.

Im Reiter **Webbrowser** können Sie festlegen, dass der Webbrowser auf dem Clientcomputer automatisch so konfiguriert wird, dass er als Proxyserver den auf der Seite **Allgemein** angegebenen ISA Server-Computer verwendet.

Verschlüsselte Firewallclientverbindungen

Der ISA Server 2004 FW-Client bietet die Möglichkeit, den Datenverkehr zwischen dem Firewallclient und dem ISA Server zu verschlüsseln. Verwenden Sie frühere Versionen der Firewallclientsoftware, so können diese FW-Clients eine Verbindung zum ISA Server 2004 aufbauen wenn Sie in der ISA Verwaltungskonsole den Haken bei **Unverschlüsselte Firewallverbindungen zulassen** setzen. Nach Aktivierung dieser Funktion erfolgt die Kommunikation zwischen FW-Client und ISA Server unverschlüsselt.

Firewallclienteinstellungen
Verbindung
Anwendungseinstellungen
Der Firewallclient für ISA Server 2004 verwendet ein Protokoll, das den Kanal zwischen dem Firewallclient und dem ISA Server-Computer verschlüsselt.
Firewallclients, die frühere Versionen der Firewallclientsoftware verwenden, werden ebenfalls unterstützt. Für diese Verbindungen wird keine Verschlüsselung verwendet.
Unverschlüsselte Firewallclientverbindungen zulassen
OK
Abbrechen
Übernehmen

ISA Server Clients - Teil 3: Der Webproxyclient

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Das Kapitel über die vom ISA Server unterstützen Clients teilt sich in drei Artikel auf:

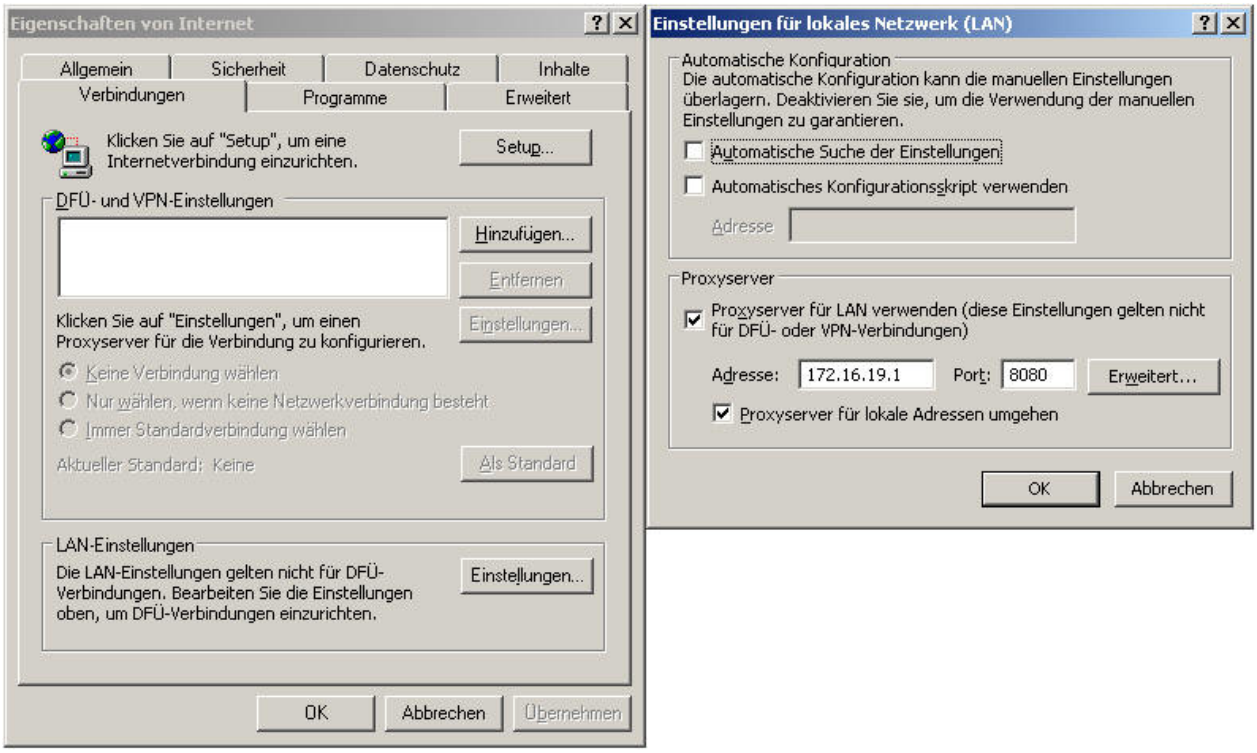
- Teil 1: Der SecureNAT-Client
- Teil 2: Der Firewallclient
- Teil 3: Der Webproxyclient

Der Webproxyclient

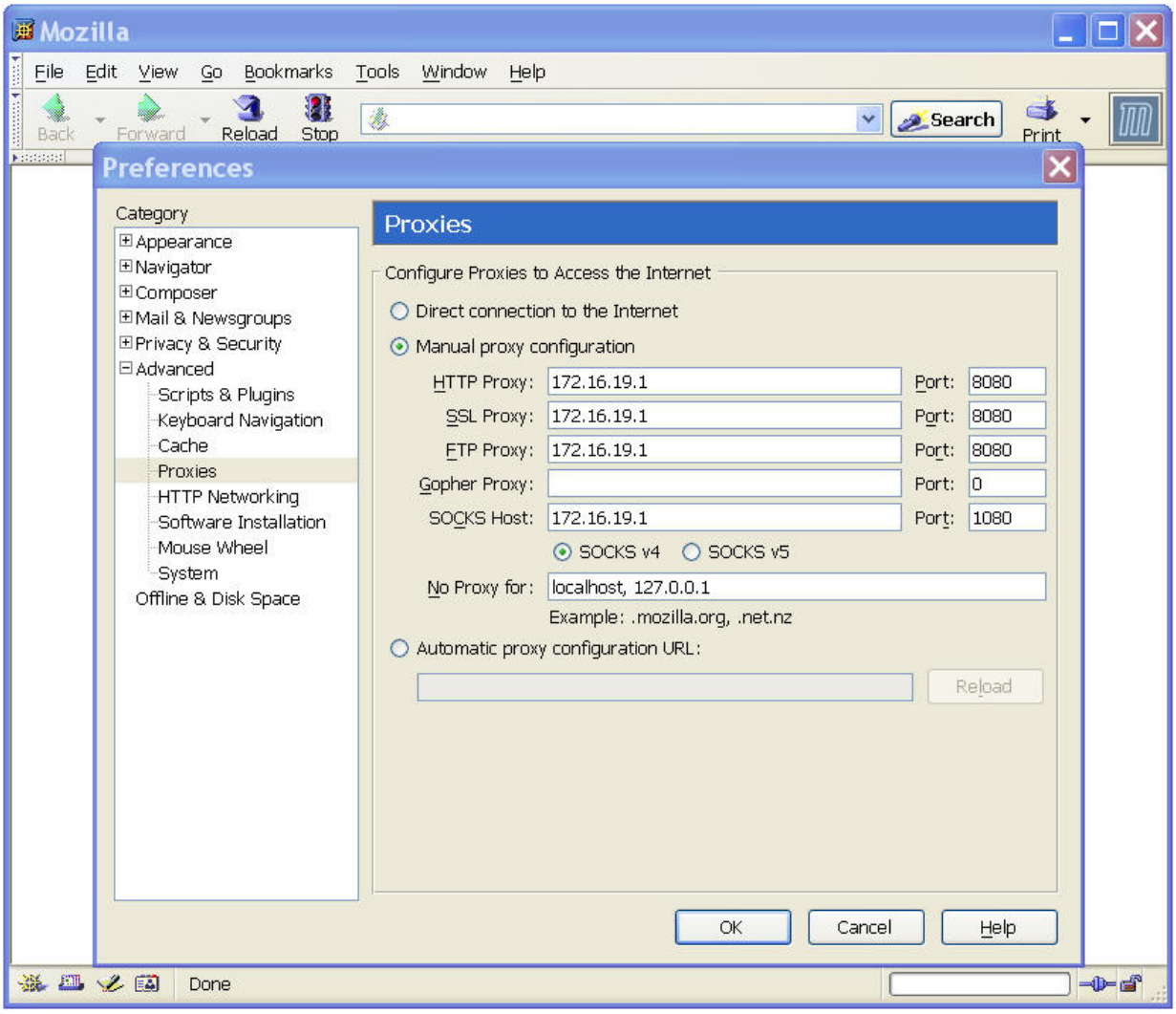
Ein Webproxyclient ist ein Clientcomputer mit einer Webbrowseranwendung, die dem Hypertext Transfer Protokoll (HTTP) 1.1 entspricht und so konfiguriert ist, dass der Webproxyfilter des ISA Server für ausgehende Webanfragen verwendet wird. Der Webproxyfilter (und somit der Webproxyclient) unterstützt die folgenden Protokolle: FTP, HTTP und HTTPS.

Es muss - wie beim SecureNAT-Client - keine Software auf dem Client installiert werden; es ist ähnlich wie bei diesem nur eine Konfigurationsangelegenheit. Dabei spielt es erstmal keine Rolle, welcher Webbrowser verwendet wird. Sämtliche HTTP 1.1 kompatible Browser (z.B. Microsoft Internet Explorer, Version 3.02 und höher sowie Netscape 2.0 und höher) unterstützen einen Proxy für ausgehende Anfragen. Lediglich wenn die Authentifizierung auf Benutzerebene verwendet werden soll, wird ein Internet Explorer benötigt um die integrierte Authentifizierung zu verwenden; der Netscape unterstützt nur Standardauthentifizierung.

Die Einstellungen können entweder an jedem Client manuell vorgenommen werden oder per Gruppenrichtlinie und ggfs. zusammen mit WPAD verteilt werden.



Konfiguration eines Internet Explorers als Webproxyclient.

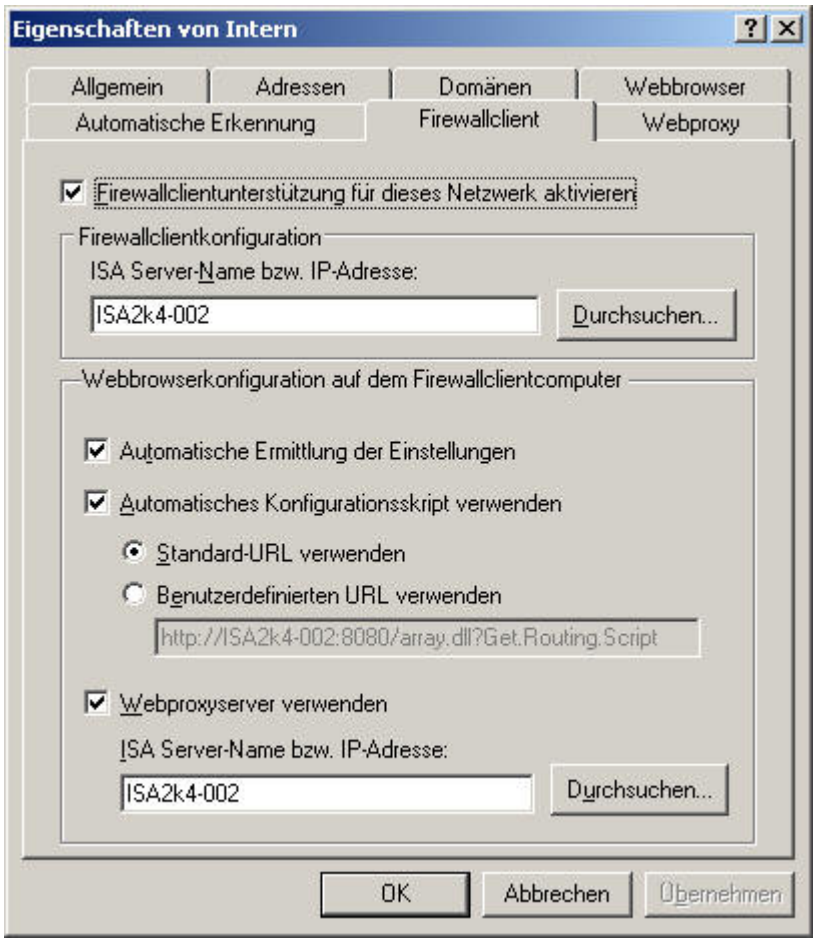


Konfiguration eines Mozilla Browser.

Tip:
Verwenden Sie die interne IP-Adresse und nicht den Computernamen oder den DNS-Namen des ISA Servers, da bei deren Auflösung die externe IP-Adresse des ISAs verwendet wird. In diesem Fall werden Anfragen vom Browser verworfen, weil die externe IP-Adresse nicht in der lokalen Adresstabelle enthalten ist und der Zugriff somit verweigert wird. Daher muss der Browser auf dem Server so konfiguriert werden, dass die Verbindung über den Webproxyfilter hergestellt wird.

Um die Einstellungen für den Webproxyclient den Clients bei der Installation des Firewallclients mitzugeben, kann dies am ISA Server eingestellt werden.

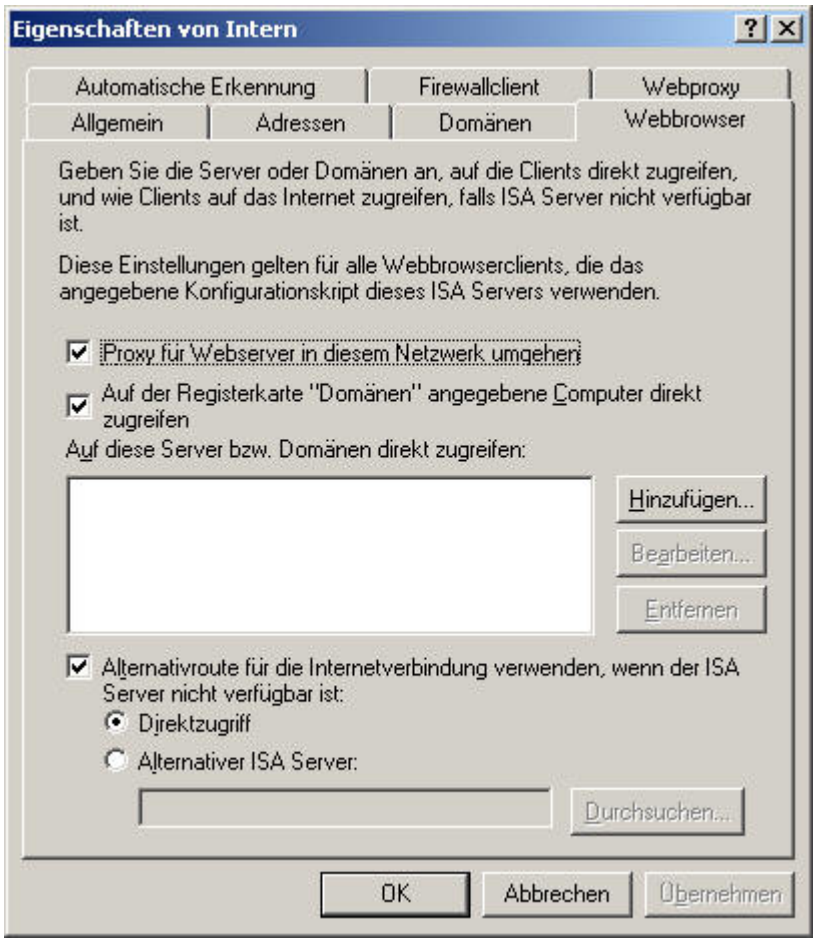
Dazu werden die Eigenschaften der Komponenten der Clientkonfiguration (ISA Verwaltungskonsole -> Netzwerke -> Intern) geöffnet:



Der Standardkonfigurations-URL lautet http://*Computername*:Port/array.dll?Get.Routing.Script, wobei *Computername* für den Namen des ISA Server-Computers und *Port* für den Port des Webproxyfilters steht. An dieser URL befindet sich das Konfigurationsskript. ISA Server erstellt dieses Skript basierend auf den Optionen für Direktzugriff und Reserveroute automatisch.

Sie können eine Option einstellen, durch die ISA Server ein Clientkonfigurationsskript, das sich auf dem ISA Server-Computer befindet, bei jedem Öffnen des Webbrowsers automatisch downloadet. Die Ausgabe dieses Skripts liefert eine geordnete Reihe von ISA Server-Computern, die der Browser zum Abrufen des durch den URL angegebenen Objekts verwendet. Verwenden Sie dazu WPAD.

In der Registerkarte "Webbrowser" können Server festgelegt werden, bei deren Zugriff der Webproxyfilter umgangen werden soll:



Wenn im Netzwerk mehrere ISA Server vorhanden sind kann über die Option "Alternativroute" festgelegt werden, welcher ISA Server angefragt werden soll, wenn der eigentliche konfigurierte ISA Server nicht erreichbar ist:

Eingehende VPN-Verbindungen per PPTP

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Wie der ISA Server 2000 unterstützt der ISA Server 2004 die VPN Einwahl durch Remoteclients.
Durch eine VPN Verbindung wird ein sicherer Tunnel über ein Netzwerk, wie das Internet, aufgebaut, über den der Client Zugriff auf Ressourcen des Firmenetzwerkes bekommt.

Vorteile einer VPN Verbindung:

- Bei vorhandener DSL Flatrate entstehen keine weiteren Kosten für die Einwahl
- Abhängig von der Internetanbindung ist eine VPN Verbindung schneller als per Telefonleitung
- Eine VPN Verbindung kann von jedem Ort aus aufgebaut werden, sobald es einen Internetzugang gibt, z.B. Flughafen

Der ISA Server 2004 unterstütz zur Remoteeinwahl per VPN die zwei Tunnelprotokolle PPTP und L2TP/IPSEC.
Das Tunnelprotokoll PPTP, auf das sich diese Anleitung bezieht, ist leicht einzurichten und hat den Vorteil, dass es
ohne Probleme mit Geräten die NAT anwenden funktioniert. L2TP/IPSEC hingegen bietet einen höheren Sicherheitstandart
als PPTP und funktioniert mittlerweile auch, durch NAT-T (NAT - Traversal), mit Geräten die NAT anwenden. Hierbei ist
allerdings zu beachten, dass der Router L2TP/IPSEC Passtrough unterstützen muss.

Die Konfiguration der VPN Remoteeinwahl erfolgt durch die, in nachstehendem Bild zu sehenden, 5 Schritte.

Die Nummerierung der einzelnen Kapitel entspricht den einzelnen Schritten auf dem Bild.

---

1. Verifizieren, dass der VPN Clientzugriff aktiviert ist

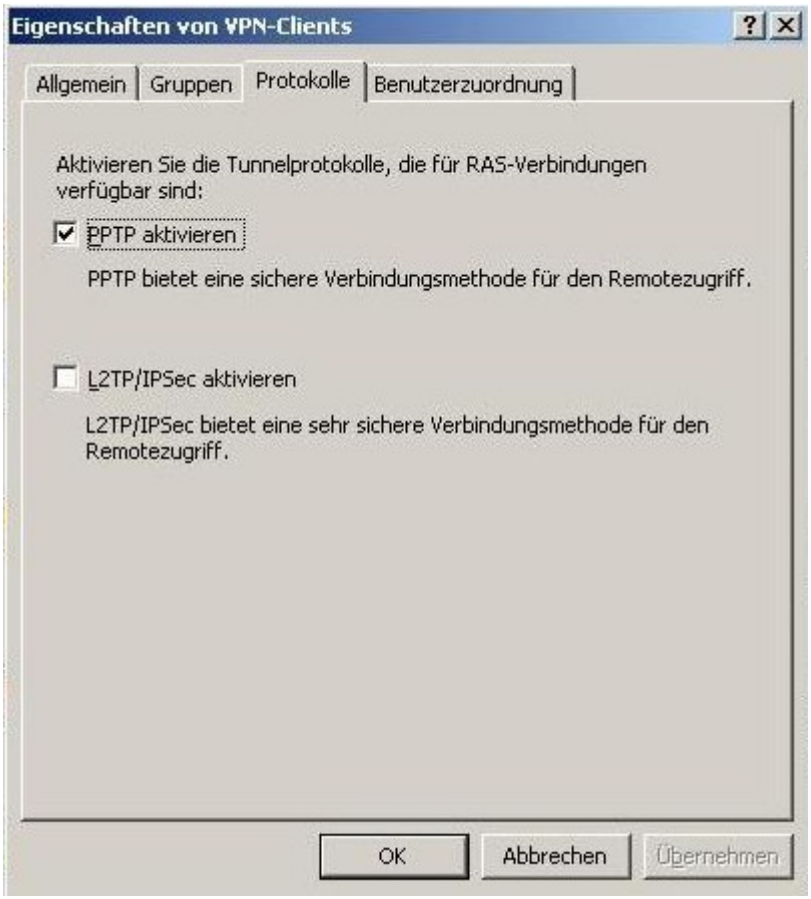
Damit der ISA Server VPN - Clientverbindungen akzeptiert muss der Haken bei *VPN ClientZugriff aktivieren* gesetzt werden. Die Option *Maximale Anzahl zugelassener VPN-Clients* legt die maximale Anzahl der gleichzeitigen Verbindungen fest. Standartmässig steht diese Option auf 5 Verbindungen. Ändern Sie diese Option auf die Anzahl der benötigten gleichzeitigen Verbindungen ab.

2. Windows Benutzer angeben

Der ISA Server 2004 erwartet eine Angabe von zugelassenen Benutzern bzw. einer Gruppe, die eine VPN Verbindung mit dem ISA Server herstellen dürfen. Die einfachste Möglichkeit ist, dies durch eine Gruppe zu realisieren, dabei ist es egal, ob es sich um eine lokale Gruppe oder eine Gruppe aus der Domäne handelt.

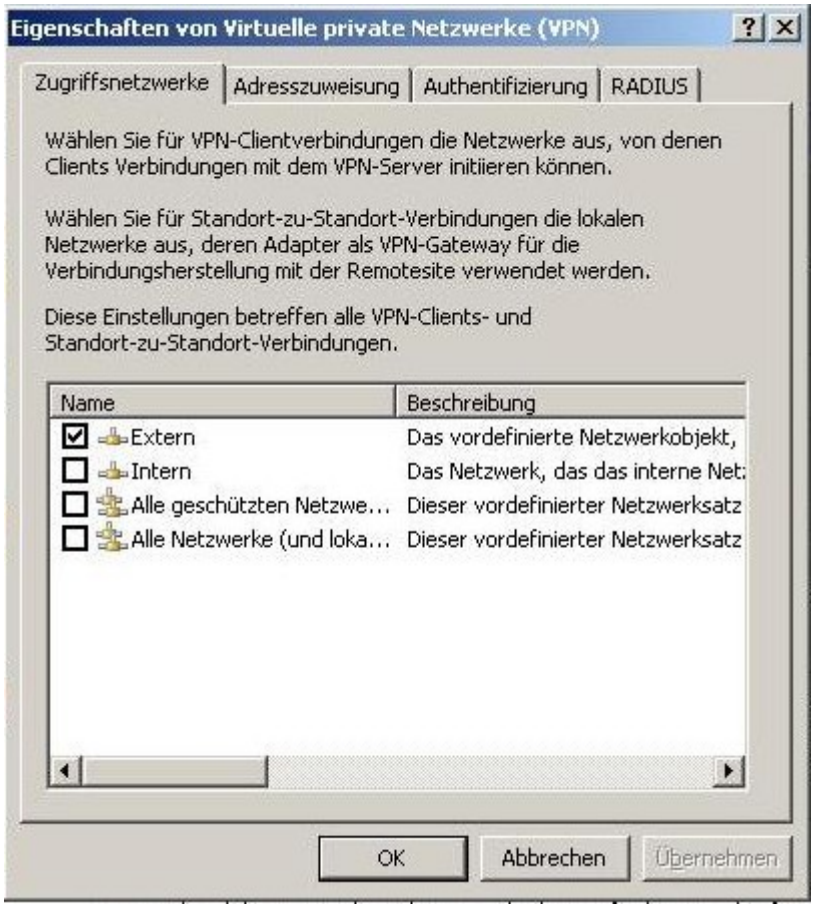
Hinweis: Alternativ ist auch eine Authentifizierung über RADIUS möglich. Falls der ISA Server kein Mitglied der Domäne sein sollte kann trotzdem mittels RADIUS eine Authentifizierung auf Domänenebene stattfinden.

3.1 VPN Eigenschaften

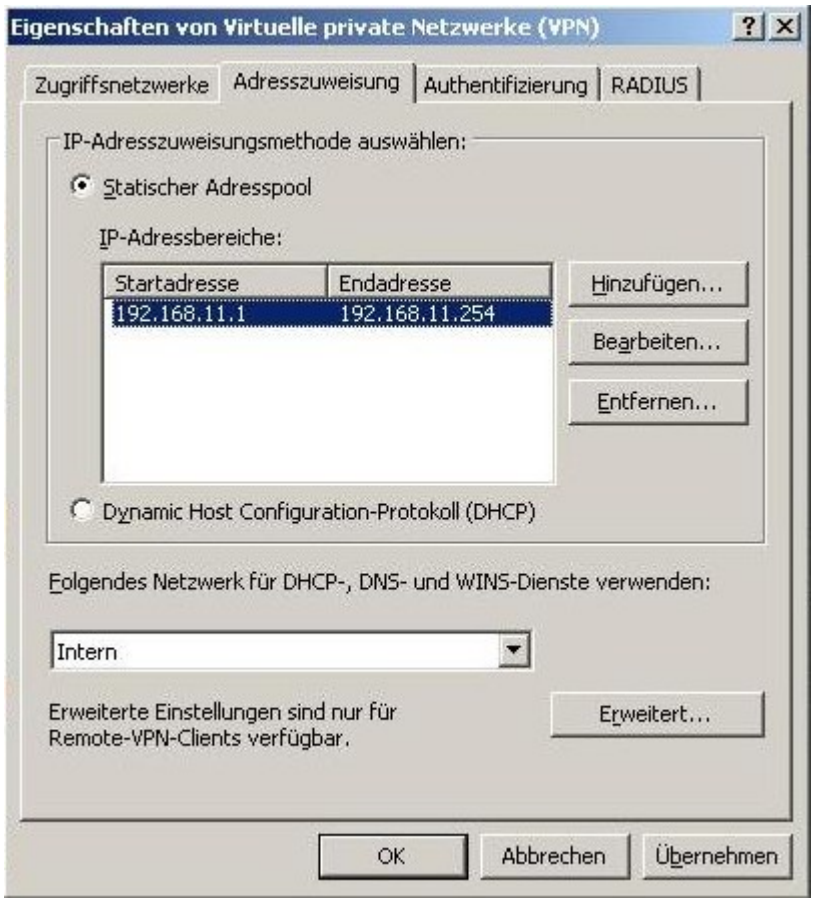


Es muss das Tunnelprotokoll ausgewählt werden, für das der ISA Verbindungen akzeptieren soll. Diese Anleitung beschränkt sich auf das Tunnelprotokoll PPTP.

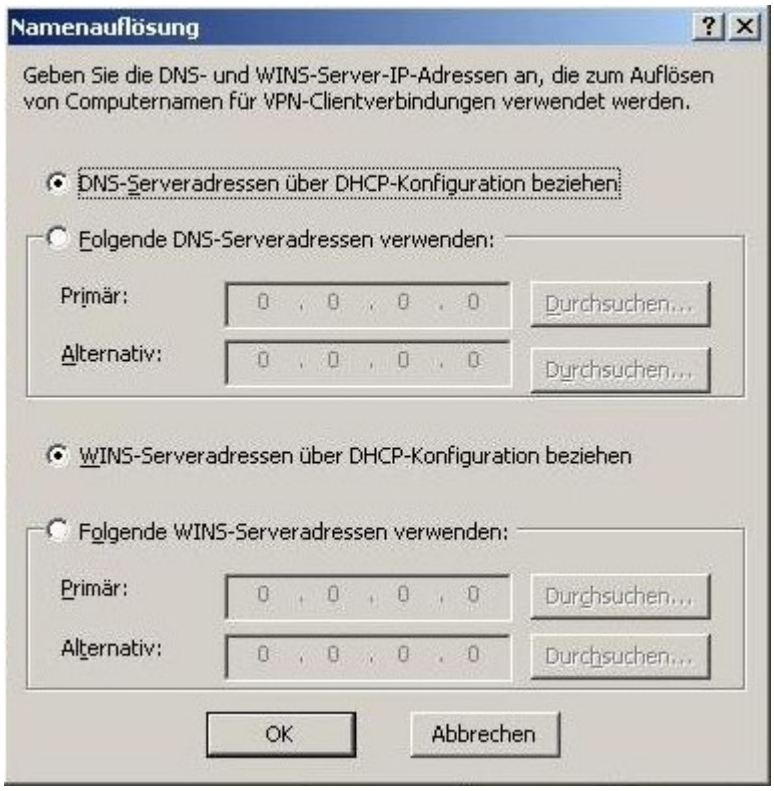
3.2 Remotezugriffskonfiguration



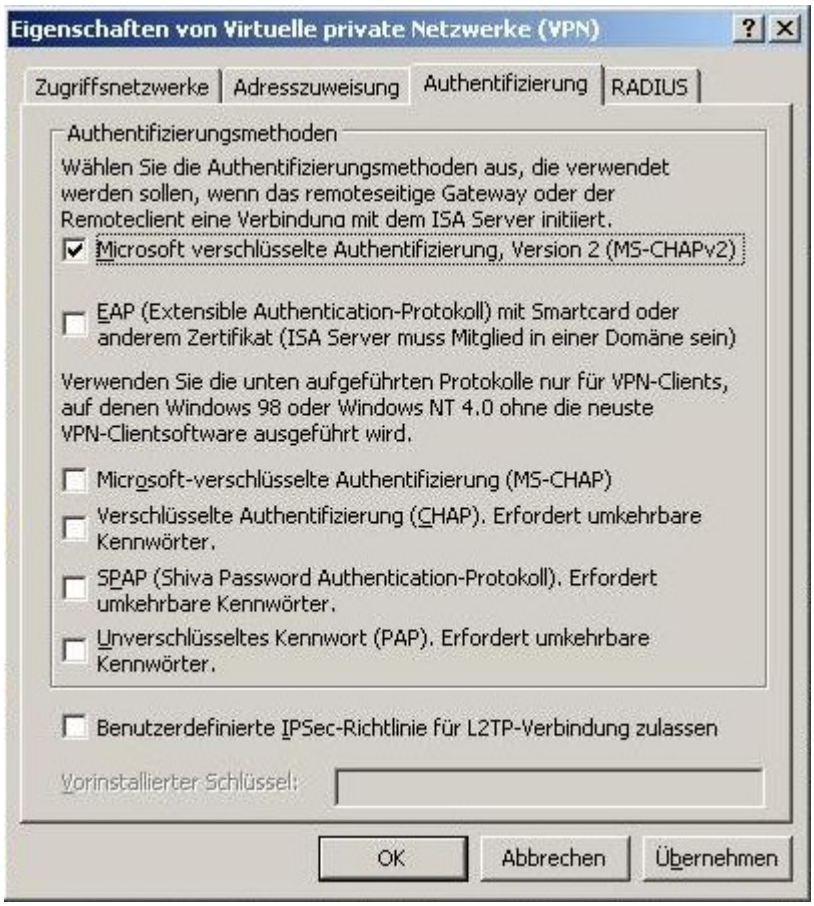
Der VPN Zugriff kann aus mehreren Netzwerken erfolgen, meistens geschieht dies aus dem Internet, hierfür muss das Netzwerk *Extern* ausgewählt sein. Sollten VPN Verbindungen aus weiteren Netzen aufgebaut werden, müssen diese hier zusätzlich angegeben werden.



Unter dem Karteireiter *Adresszuweisung* wird festgelegt, wie die VPN Clients ihre IP Adresse beziehen. Es besteht die Möglichkeit durch einen statischen Adresspool oder durch einen DHCP Server. Die Option *Folgendes Netzwerk für DHCP-, DNS-und WINS Dienste verwenden* ist dafür verantwortlich welche DNS- und WINS Server dem VPN Client zugewiesen werden. Diese Einstellungen können unter dem Punkt Erweitert, wie im nächsten Bild zu sehen, auch manuell konfiguriert werden.



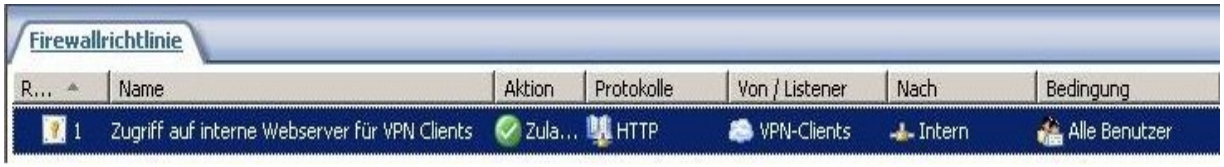
Die DNS- und WINS Server können hier angepasst werden, falls eine alternative Konfiguration nötig ist.



Für den Verbindungsaufbau muss eine Authentifizierungsmethode angegeben werden, mit der

sich der Remotebenutzer authentifizieren muss. Sinnvoll ist es dies bei der Authentifizierungsmethode MS-Chap V2 zu belassen, da dies die sicherste der angebotenen Methoden für Authentifizierung mit Benutzername und Kennwort ist.

4. Firewallrichtlinie für das Clientnetzwerk anzeigen

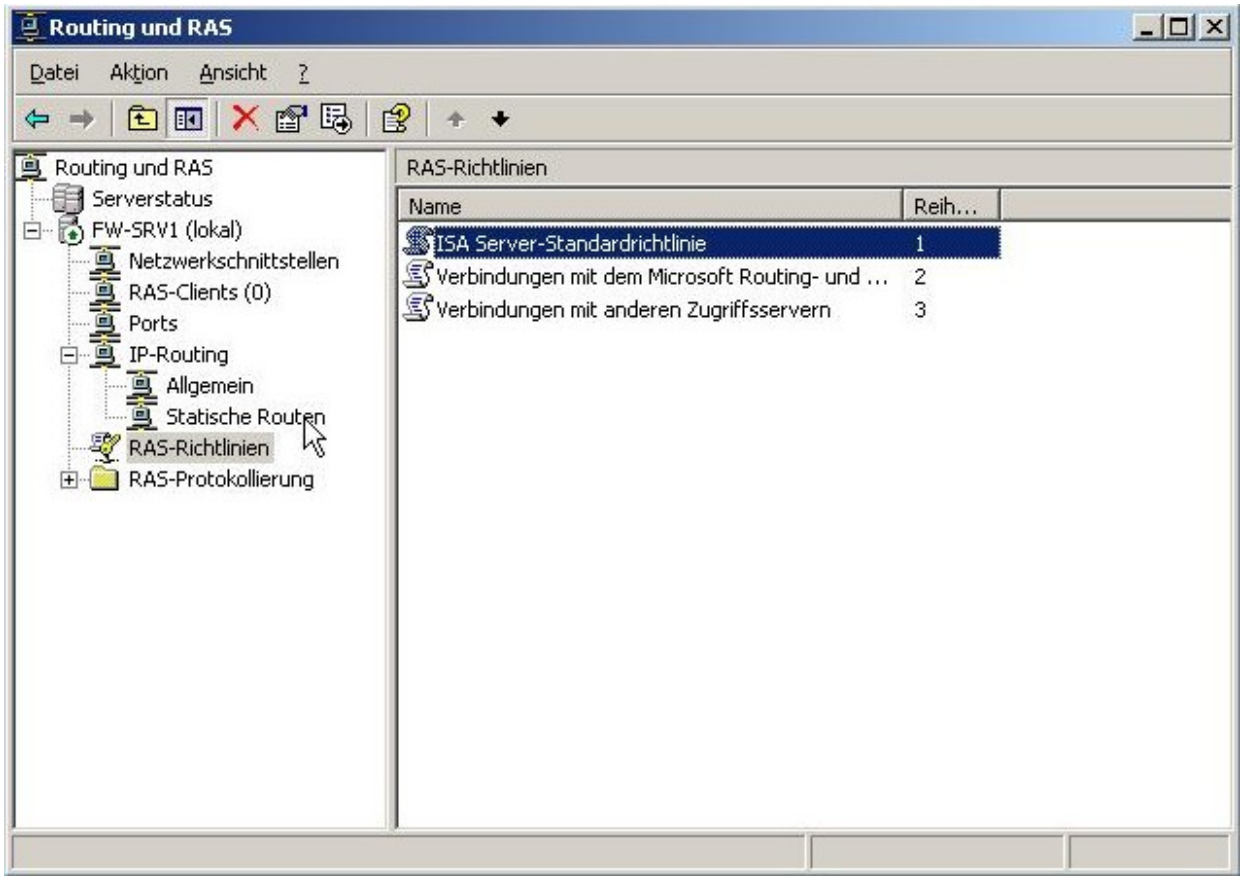


Abschließend muss noch eine Regel bzw. Regeln erstellt werden, die den VPN Clients Zugriff auf das interne Netzwerk gewährt.
Neu beim ISA 2004 ist, dass der Zugriff auf bestimmte Protokolle und interne Server eingeschränkt werden kann. Obige Regel erlaubt z.B. nur Zugriff von VPN Clients auf interne Webserver per HTTP.

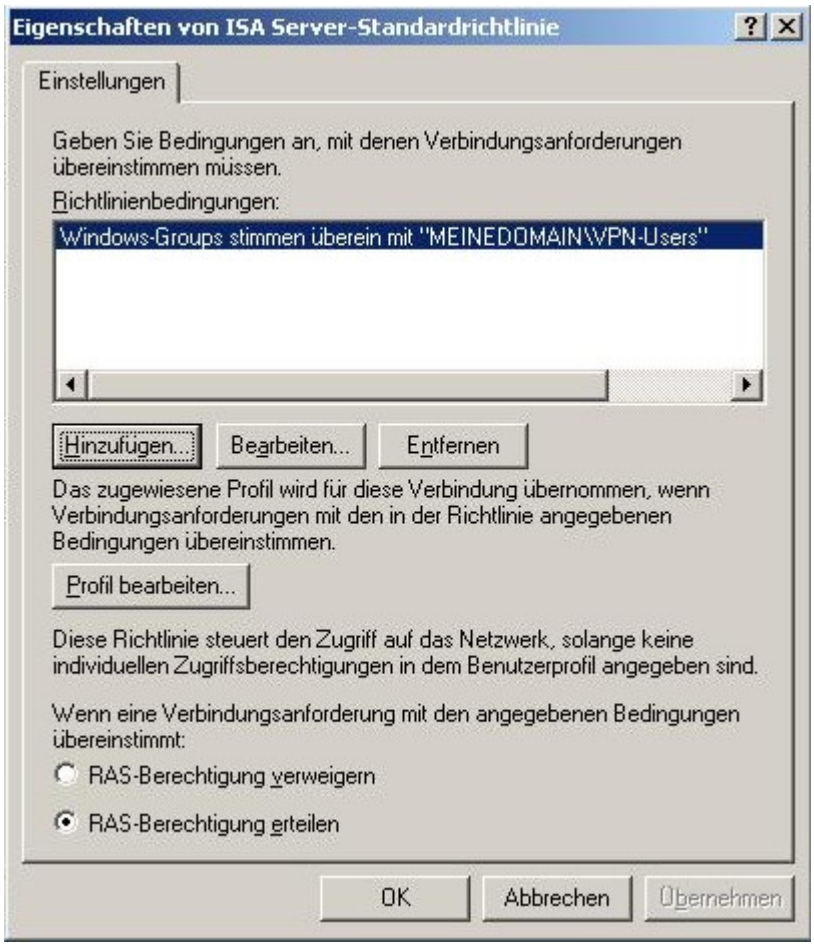
5. Netzwerkregeln anzeigen

Falls es nötig sein sollte kann hier die Beziehung zwischen den Netzwerken konfiguriert werden, d.h. ob von dem VPN Client-Netzwerk in andere Netzwerke geroutet oder NAT angewandt werden soll.

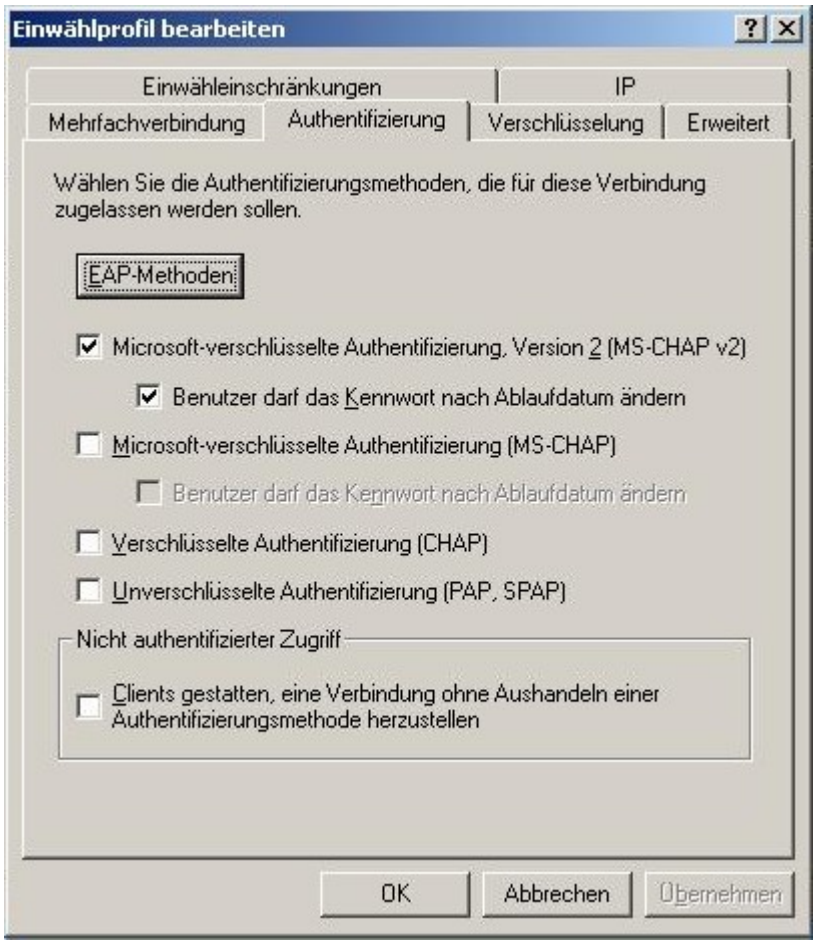
6. Was passierte durch die Konfiguration der Punkte 1 - 3



Durch die eben durchgeführten Schritte wurde im Routing und RAS Dienst eine neue RAS Richtlinie, *ISA Server Standardrichtlinie* erstellt.



Wie angegeben werden Einwahlberechtigungen nur für Mitglieder der Gruppe VPN-Users erteilt. Bei Bedarf kann die Richtlinie mit weiteren Bedingungen, wie z.B. durch einen Zeitraum in dem sich Benutzer einwählen dürfen, erweitert werden.



Die Authentifizierungsmethode wurde nur auf MS-Chap V2 gesetzt.

ISA Server 2004 – Site–to–Site VPN mit L2TP/IPSec

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

Dieser Artikel beschreibt die Einrichtung eines Site to Site VPN Netzwerkes zwischen zwei mit SDSL ans Internet angebundenen Standorten Obernkirchen (OBK) und Braunschweig (BS). Beide Standorte verwenden einen ISA Server 2004 Standard.

Überblick über Site to Site VPN

Große Unternehmen verfügen häufig über mehrere Standorte, die untereinander kommunizieren müssen, z. B. eine Unternehmenszentrale in Obernkirchen München und eine Schulungsniederlassung in Braunschweig. Die beiden Standorte können mithilfe eines Site to Site VPN sicher über das Internet verbunden werden.

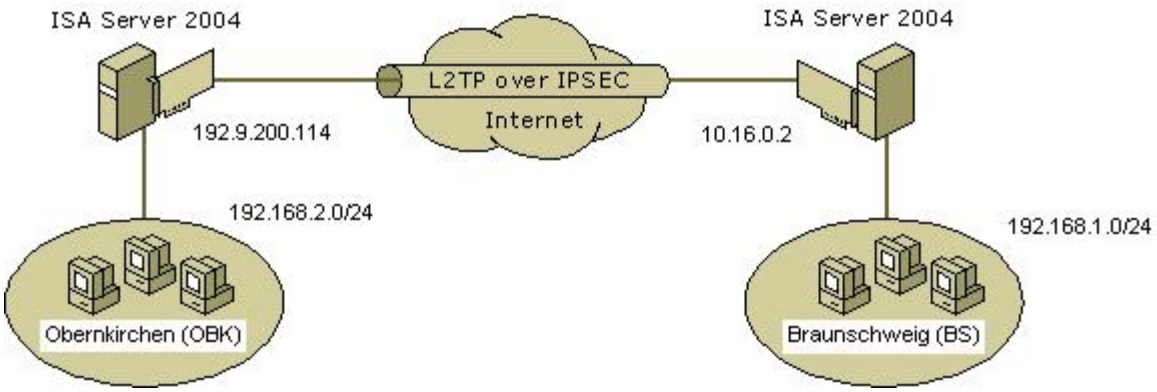
ISA Server 2004 enthält drei VPN-Protokolle für Site to Site Verbindungen:

- PPTP (Point-to-Point Tunneling-Protokoll)
- L2TP (Layer 2 Tunneling-Protokoll) über IPSec (IP Security)
- IPSec-Tunnelmodus (IP Security-Protokoll)

Die Verfahren zum Konfigurieren von Remote-VPN-Netzwerken unterscheiden sich je nach ausgewähltem Tunneling-Protokoll. Bei allen Remotestandortnetzwerken muss das Netzwerk konfiguriert, eine Netzwerk- und Firewallrichtlinie für das Remotenetzwerk eingerichtet und das Remotestandortgateway (VPN-Server) konfiguriert werden.

Für IPSec-Netzwerke können darüber hinaus die Sicherheitseinstellungen auf dem ISA Server 2004 Computer konfiguriert werden. Außerdem müssen die IPSec-Richtlinieneinstellungen auf dem Remotestandortgateway konfiguriert werden.

Ein Site to Site VPN mit IPSEC sollte nur aus Abwärtskompatibilitätsgründen mit anderen Firewalllösungen verwendet werden. Site to Site VPN mit IPSEC ist auch ein neues Feature des ISA Server 2004.



Starten Sie mit der Erstellung des S2S VPN auf dem ISA Server in Obernkirchen.

Zur Erstellung eines Site to Site VPN starten Sie die ISA Server Verwaltungskonsole und klicken Sie unterhalb des ISA Server Firewallobjektes auf virtuelle private Netzwerke (VPN) und dort auf den Reiter Remotestandorte.

Dort klicken Sie auf der rechten Seite in den Remotestandortaufgaben auf Remotestandortnetzwerk hinzufügen.

Folgen Sie den Anweisungen des Assistenten und vergeben einen Namen für den Remotestandort.

Als Protokoll wählen Sie L2TP über IPSec. Dabei handelt es sich um das zurzeit bevorzugte Protokoll für eine VPN / Site to Site Verbindung.

Im folgenden Fenster müssen Sie die IP Adresse oder den Namen des Remote VPN Servers angeben.

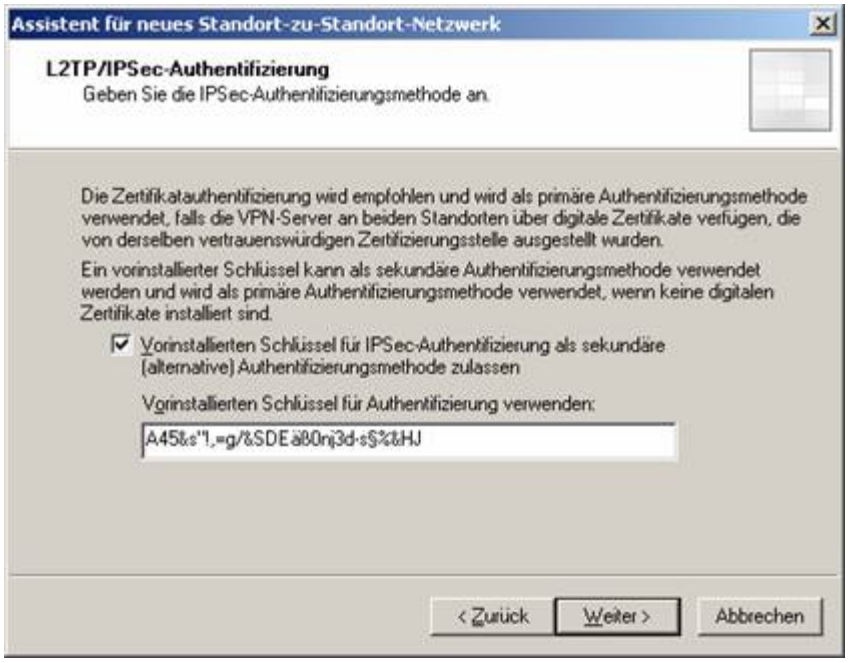
Bemerkung: Bei nicht statischen IP Adressen müssen Sie hier Verfahren wie DYNDNS einsetzen und im Remotestandortgateway einen Namen angeben (z. B. ISA-Remote.dyndns.org)

Soll der lokale Standort Verbindungen mit dem Remote Standort aufbauen dürfen, geben Sie in folgender Dialogbox den Benutzernamen, Domänennamen und das Kennwort für die Verbindung an.

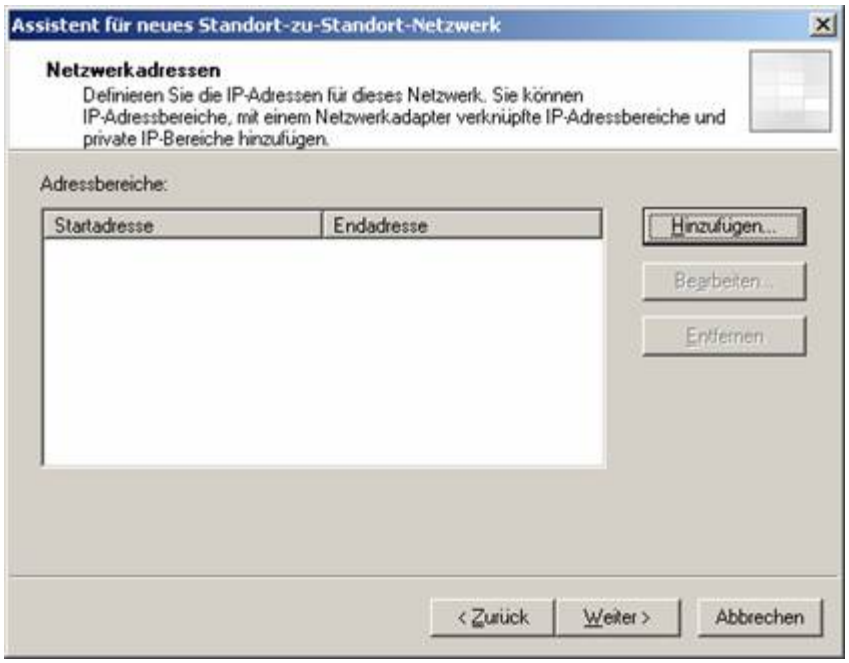
Für eingehende Verbindungen müssen Sie auf dem ISA Server Computer einen Benutzer definieren, welcher mit dem Namen des Remotestandortnetzwerkes übereinstimmen muss. Dieser Account muss auch das Recht zur Remoteeinwahl haben (Das Benutzerkonto wird am Ende des Artikels gezeigt).

In großen Umgebungen mit zahlreichen Standorten ist es sinnvoll, eine Zertifikatauthentifizierung einzurichten. Hierfür ist jedoch die Einrichtung einer Inhouse Zertifizierungsstelle erforderlich, welche jedoch sehr viel Verwaltungsaufwand erfordert. In unserem Beispiel verwenden wir keine Zertifizierungsstelle sondern einen vorinstallierten Schlüssel zur Authentifizierung, den so genannten Preshared Key.

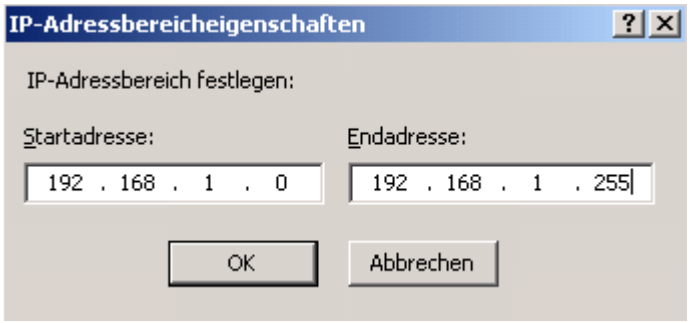
Verwenden Sie für den PSK (Pre Shared Key) eine sehr komplexe, lange und zufällige Zeichenfolge wie in diesem Beispiel.



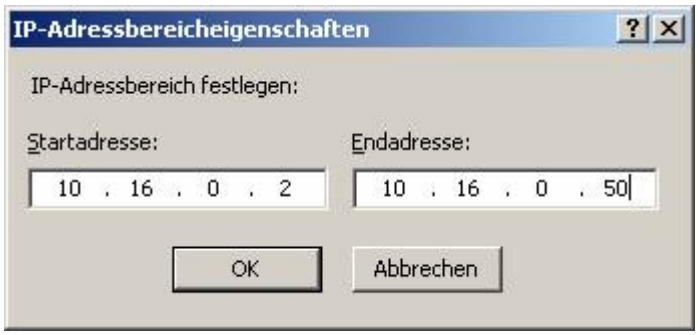
Für das Site to Site Netzwerk müssen Sie jetzt noch den internen IP-Adressbereich der Clients hinter dem Remote ISA Server angeben (Standort Braunschweig (BS)).



Geben Sie hier den Adressbereich ein.



Geben Sie zusätzlich noch die IP-Adresse des externen Interface des Remote ISA Server an. Diese Einstellung ist notwendig, damit Web Proxy Clients auf das Netzwerk zugreifen können.



Die Konfiguration ist beendet. Sie können den Assistenten fertig stellen.

Schritte zur Netzwerkkonfiguration

Damit neu erstellte Netzwerke Datenverkehr senden oder empfangen können, müssen weitere Konfigurationsschritte durchgeführt werden. Diese Schritte sind vom Typ des erstellten Netzwerks abhängig. Wir konzentrieren uns auf das Site to Site Netzwerk mit L2TP.

Site to Site VPN mit L2TP

Damit Clients eine Verbindung aus dem VPN über PPTP (Point-to-Point Tunneling-Protokoll) oder L2TP (Layer Two Tunneling-Protokoll) herstellen können, müssen Sie die folgenden Schritte durchführen:

- Erstellen Sie einen Benutzer mit dem Namen des neuen Netzwerks. Geben Sie dann für die RAS-Berechtigungen Zulassen an.
- Erstellen Sie Netzwerkregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.
- Erstellen Sie Zugriffsregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.

Erstellen eines Benutzers

Bei der Erstellung eines Benutzer ist der Reiter Einwählen wichtig. Dort muss dem Account der Zugriff gestattet werden.

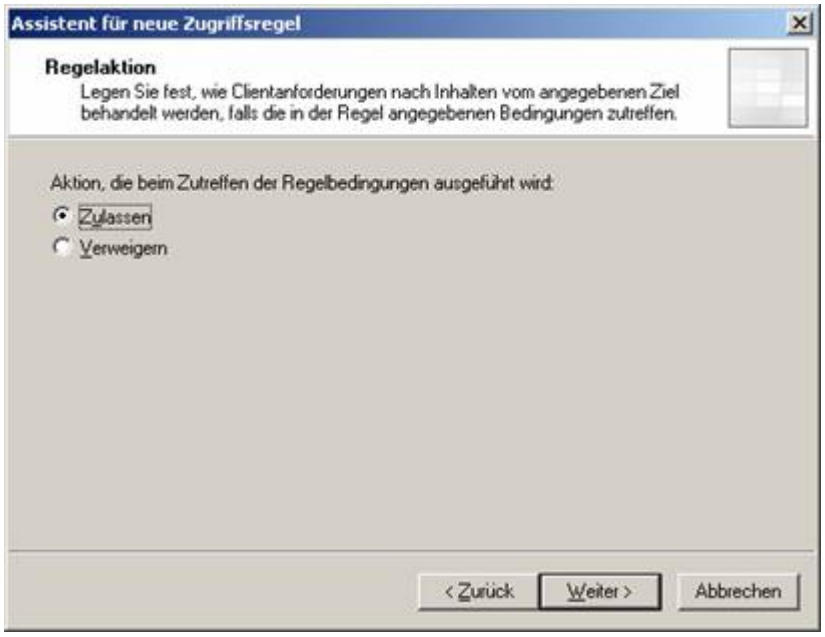
Erstellen von Zugriffsregel

Da es sich bei einem Site to Site VPN in der Regel um ein und dieselbe Firma handelt, ist es nicht notwendig, den Datenverkehr einzuschränken. Wir erstellen eine Regel mit vollständigem Zugriff.

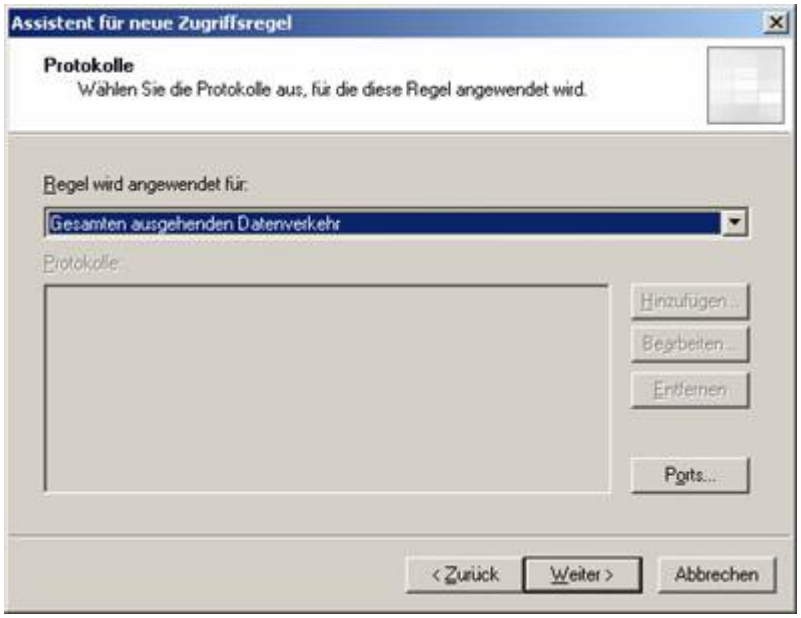
Hinweis: Sie müssen eine Zugriffsregel in beide Richtungen des jeweiligen Remotestandortes erstellen.

Achten Sie bei der Erstellung eines Site to Site VPN mit Partnern, Lieferanten usw. auf ein angepasstes Firewallregelwerk.

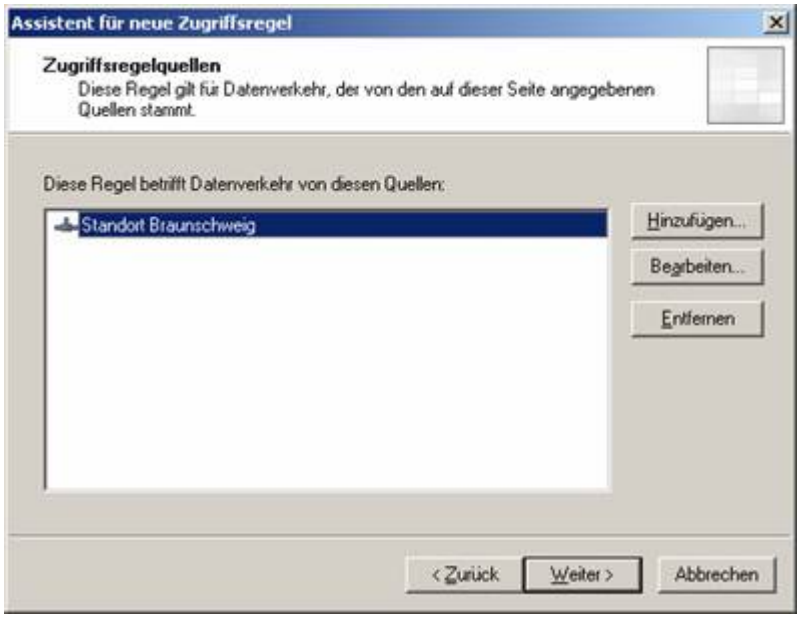
Wir erstellen eine Zulassungsregel



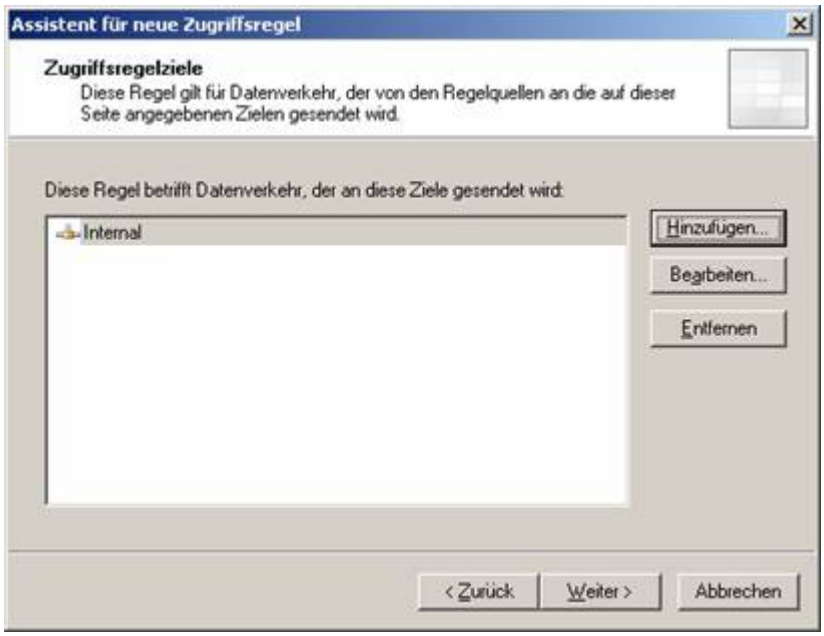
Die Regel wird für den gesamten ausgehenden Datenverkehr angewendet.



Die Regel betrifft den Datenverkehr vom Standort Braunschweig nach …



Internal



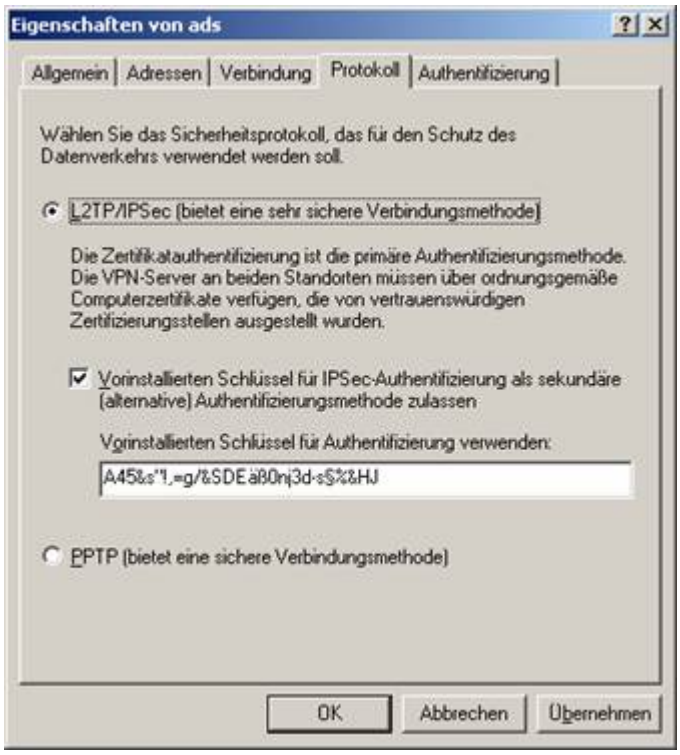
Die Regel betrifft Anforderungen von folgenden Benutzersätzen All Users.

Der Remotestandort ist jetzt konfiguriert.

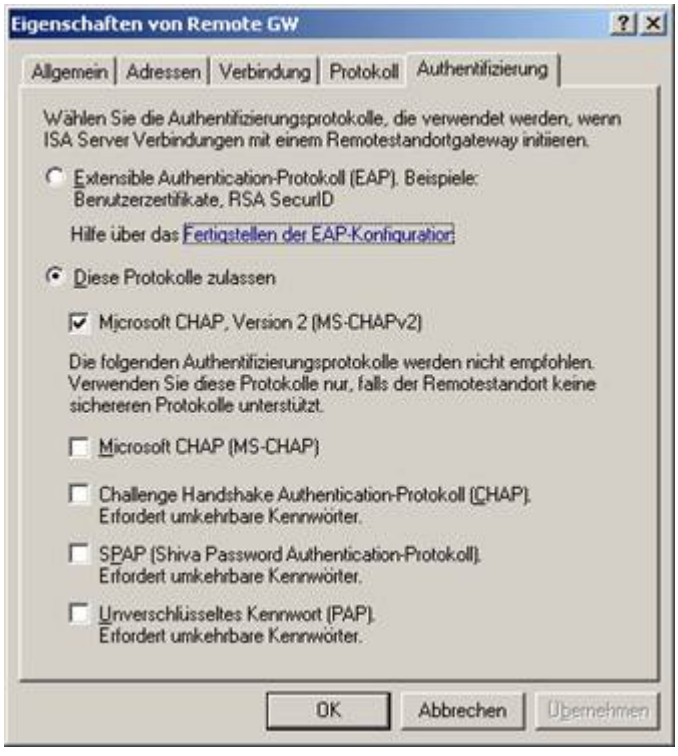
Überprüfen Sie noch einmal die Einstellungen.

Im Reiter Verbindungen können Sie noch einmal die Verbindungsdaten überprüfen und eine Beendigung der Verbindung nach Anzahl X Minuten / Stunden festlegen.

Hier können Sie das VPN Protokoll einstellen und den PSK ändern (Vorsicht: Muss auf beiden Seiten geändert werden).



Im Reiter Authentifizierung können Sie die Authentifizierungsprotokolle festlegen. PPTP/L2TP erfordern im Gegensatz zu IPSEC eine Authentifizierung.

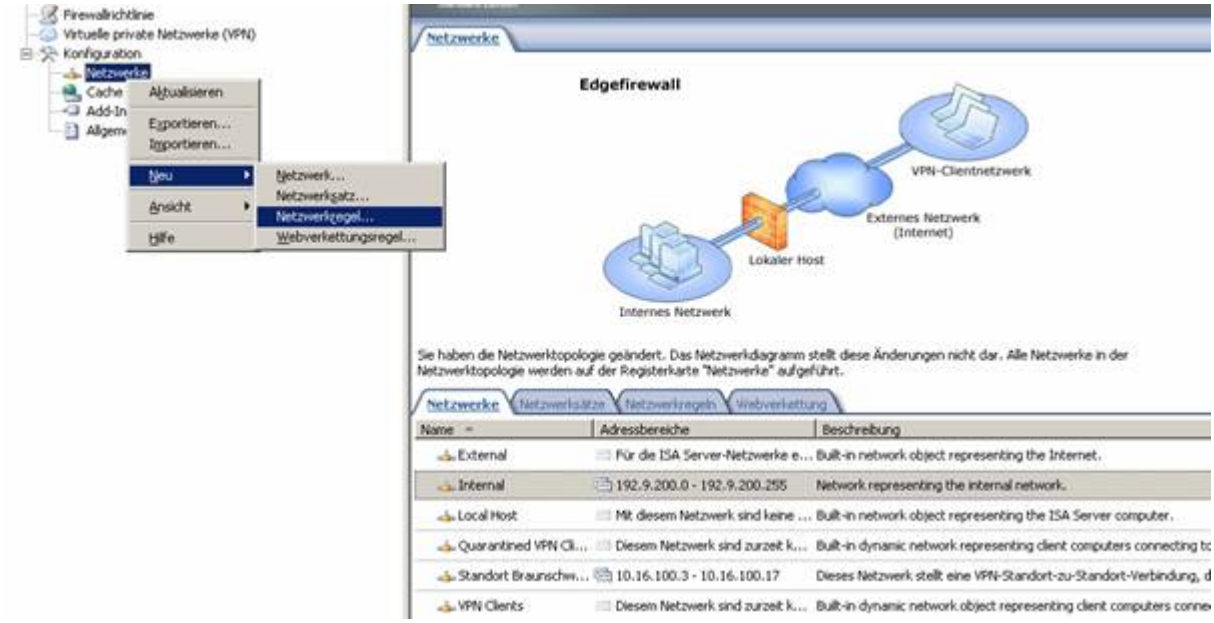


Erstellen eine Netzwerkregel

Hinweis: Da es sich bei der Netzwerkregel um eine Routingregel handelt, ist keine zusätzliche Netzwerkregel in die andere Richtung notwendig. Bei einer Netzwerkregel mit NAT hingegen

wird nur eine einseitige Verbindung erstellt.

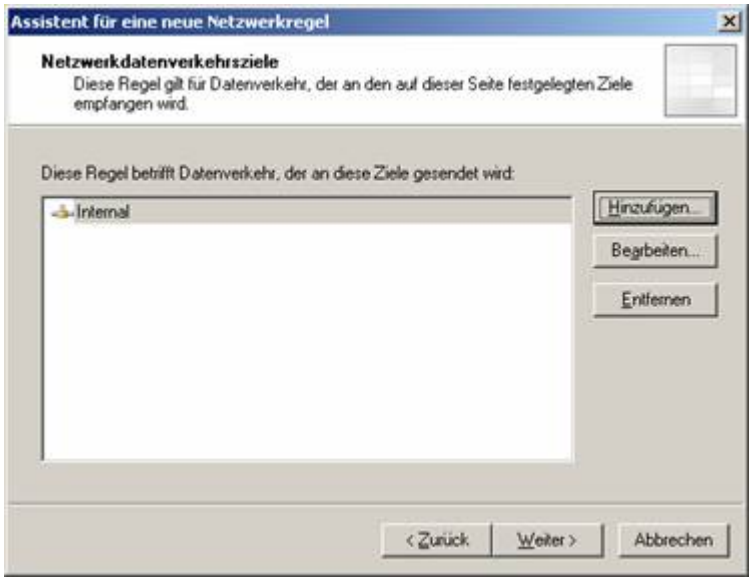
Der letzte Schritt ist die Erstellung einer Netzwerkregel, welche die beiden Standorte mit einander verbindet.



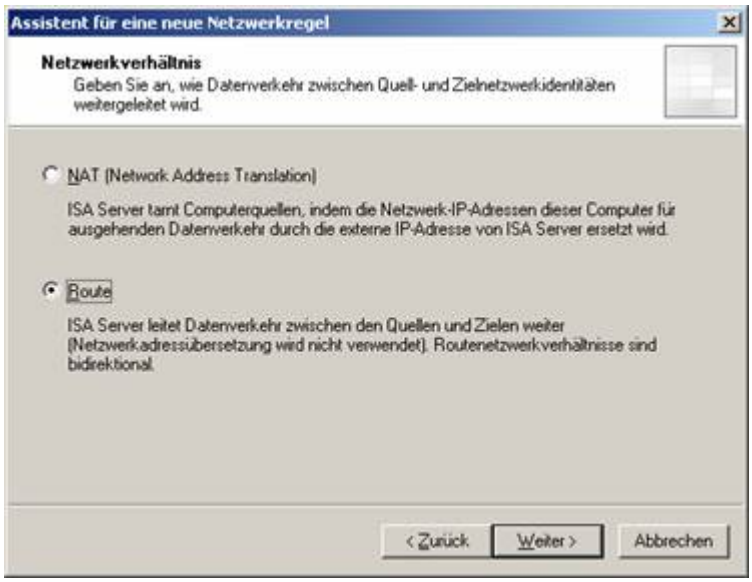
Folgen Sie den Anweisungen des Wizard und vergeben Sie einen Namen für die Netzwerkregel.

Die Regel betrifft als Source den Standort Braunschweig

Netzwerkziel ist Internal



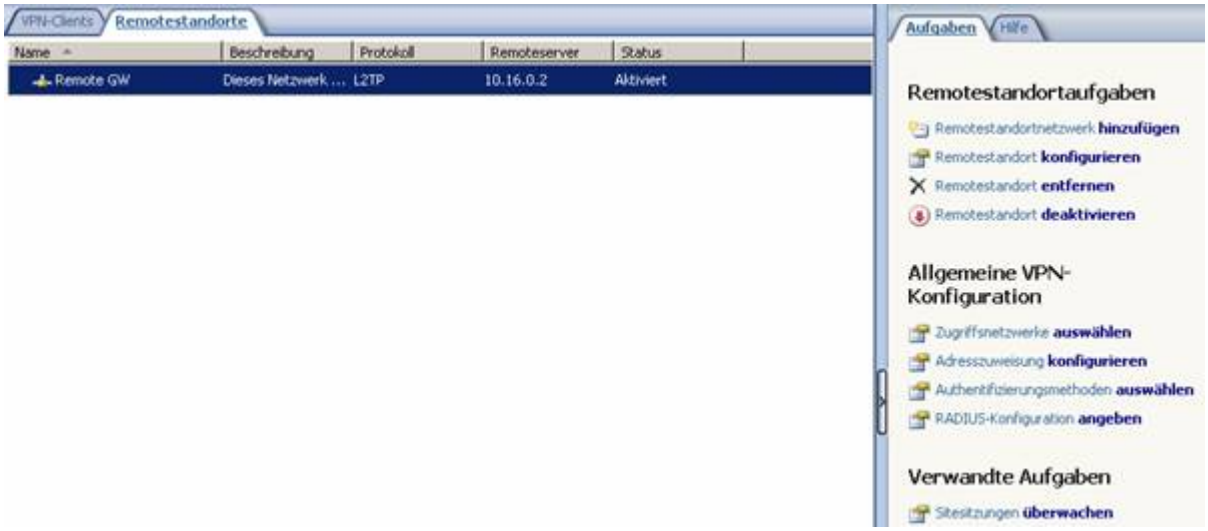
Das Netzwerkverhältnis muss auf Route stehen, da die Pakete nicht geNATet werden.



Überprüfen Sie noch einmal alle Einstellungen und beenden dann den Assistenten.

So sieht die neu erstelle Netzwerkregel aus.

Sie können die Verbindungen von und zum Remotestandort überwachen, indem Sie auf der rechten Seite im Aufgabenfenster unter Verwandte Aufgaben Sitesitzungen überwachen anklicken. Die Daten werden dann im Protokollfenster angezeigt.



ISA Server 2004 – VPN Client Zugang mit PPTP

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

Remote-VPN-Clientzugriff

Mit dem ISA Server 2004 können Sie Ihren Mitarbeitern den weltweiten Zugriff auf interne Netzwerkressourcen über eine Internetverbindung ermöglichen. Wenn sich Ihr Unternehmen beispielsweise in Obernkirchen befindet, ein Mitarbeiter jedoch in Braunschweig arbeitet, muss der Verkäufer nicht nach Obernkirchen reisen, um eine direkte Verbindung mit dem internen Netzwerk herzustellen. Stattdessen kann er über einen lokalen Internetprovider eine VPN-Verbindung aufbauen um auf das interne Netzwerk zugreifen zu können.

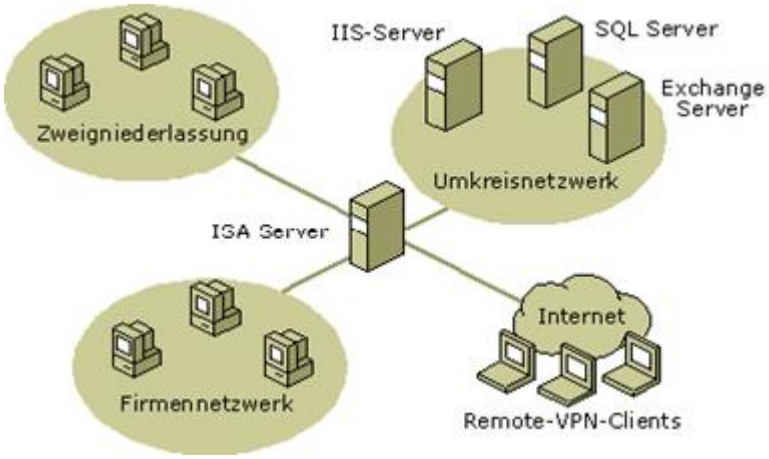
Mit dem ISA Server können Sie Lösungen für einen Remoteclientzugriff über …

- PPTP (Point-to-Point Tunneling Protocol) und
- L2TP (Layer Two Tunneling Protocol)

realisieren.

Die nächste Grafik zeigt eine typische Netzwerktopologie für Remote-VPN-Clients. In der Abbildung werden drei Netzwerke dargestellt:

- Das Internet, in dem sich der VPN-Client befindet
- Das VPN-Gateway, ein ISA Server-Computer
- Das interne Netzwerk, das einen DHCP-Server für die Zuweisung dynamischer IP-Adressen und (optional, bei Verwendung des L2TP-Tunneling-Protokolls) eine Zertifizierungsstelle enthalten kann



In unserem Beispiel verwenden wir eine VPN Client Konfiguration über das Microsoft PPTP Protokoll. Das PPTP Protokoll ist nicht ganz so sicher wie das L2TP Protokoll über IPSEC, lässt sich jedoch wesentlich leichter implementieren, weil es keine Zertifizierungsstellen-Infrastruktur mit Zertifikaten voraussetzt, wie das bei L2TP über IPSEC der Fall ist und bietet bei der Verwendung von „sicheren“ Kennwörtern in der Regel ein ausreichendes Schutzniveau.

PPTP ist auch NAT (Network Address Translation) fähig, das heißt, es existiert ein NAT Editor für PPTP.

Eine Implementierung von L2TP/IPSEC über NAT ist etwas aufwändiger, da hier NAT-T (Network Address Translation Traversal) verwendet werden muss.

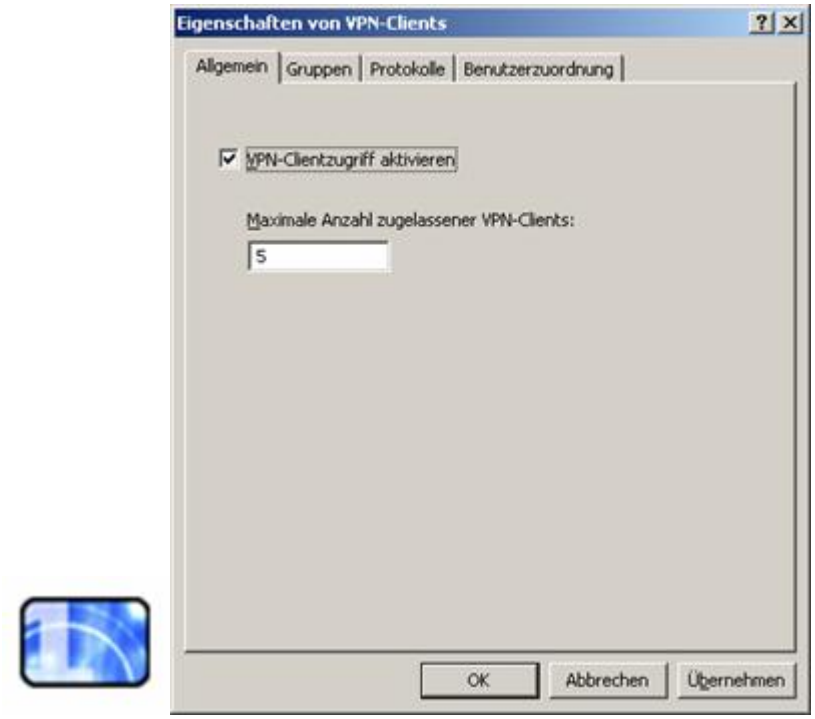
Die Implementierung einer Client VPN Verbindung über L2TP/IPSEC wird in einem späteren Artikel auf dieser Webseite beschrieben.

Zur Konfiguration des ISA Server 2004 für einen VPN Client Zugriff starten Sie die ISA Verwaltungskonsole.

ISA Server 2004 bietet einen VPN Clientzugriffs Wizard, der Sie durch die notwendigen Schritte zur Einrichtung eines Client Zugriffs führt.

Sie können den VPN-Clientzugriff über die Aufgabenleiste aktivieren.

Im ersten Schritt muss der VPN-Clientzugriff aktiviert werden. Geben Sie hier die Anzahl der maximal zugelassenen VPN Clients an.

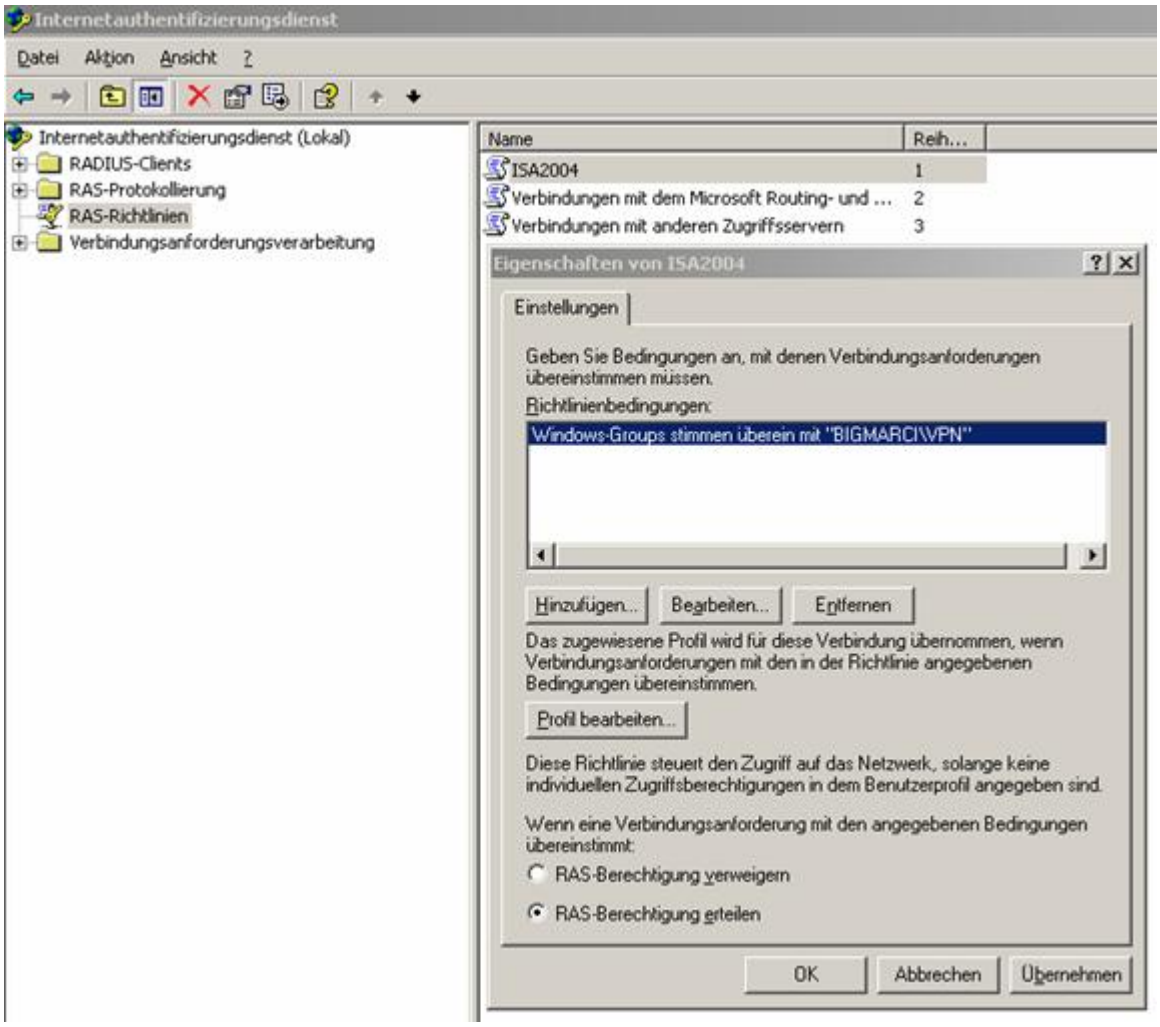


Als nächstes müssen Sie festlegen, welche Benutzer oder Gruppen für den Remotezugriff zugelassen sind. Es ist empfohlen den Remotezugriff über Windows Gruppen zu regeln. In unserem Beispiel haben wir eine Windows Gruppe mit dem Namen *VPN* erstellt und die entsprechenden Benutzer in diese Gruppe aufgenommen.

Benutzerkonten, welche sich in der Gruppe VPN befinden, muss der Remotezugriff über eine RAS-Richtlinie erlaubt sein oder der Zugriff in den Eigenschaften des Benutzerkontos aktiviert sein.

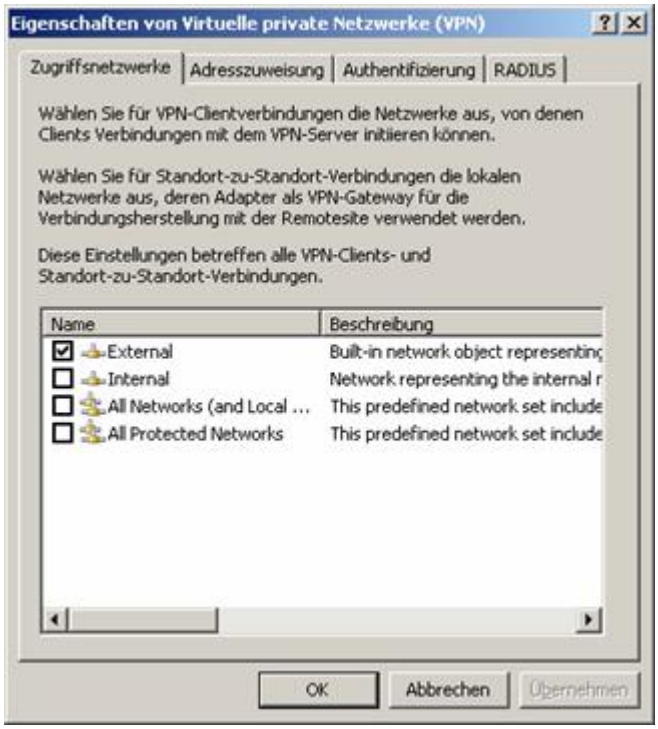
Zugriff über die Eigenschaften des Benutzerkontos aktivieren.

Zugriff über eine RAS-Richtlinie aktivieren.



Im dritten Schritt ist es notwendig, die Tunnelprotokolle auszuwählen, welche für die VPN Verbindungen verfügbar sind. Wählen Sie hier nur die Protokolle, welche Sie wirklich verwenden wollen.

Wählen Sie für VPN Clientverbindungen die Netzwerke aus, von denen Clients Verbindungen mit dem VPN-Server initiieren können. Stellen Sie sicher, dass das Netzwerk *External* ausgewählt ist.



Überprüfen Sie, ob die vom ISA Server erstellte Systemrichtlinie korrekt ist.

Zur Anzeige der Systemrichtlinie klicken Sie in der ISA Verwaltungskonsole mit der rechten Maustaste auf *Firewallrichtlinie* und wählen im Kontextmenü *Ansicht – Systemrichtlinienregeln anzeigen.*

Wenn Sie den VPN-Clientzugriff aktivieren, wird die Systemrichtlinienregel VPN-Clientdatenverkehr zu ISA Server zulassen aktiviert. Je nachdem, welche Protokolle Sie für den Remoteclientzugriff konfiguriert haben, lässt die Systemrichtlinienregel die Verwendung von PPTP (Point-to-Point Tunneling-Protokoll), L2TP (Layer Two Tunneling-Protokoll) oder von beiden Protokollen vom externen Netzwerk (vermutlicher Aufenthaltsort der VPN-Clients) zum ISA Server-Computer (lokaler Host) zu.

VPN Protokoll

Für den VPN-Clientzugriff können die Protokolle PPTP, L2TP oder beide verwendet werden. Beim Ändern dieser Einstellung wird die Systemrichtlinienregel entsprechend aktualisiert und lässt das angegebene Protokoll zu.

ISA Server fungiert für VPN-Clients als ARP-Proxy (Address Resolution-Protokoll). Wenn beispielsweise dem VPN-Clientnetzwerk zugewiesene Adressen Bestandteil des internen Netzwerksegments sind, senden Computer des internen Netzwerks ARP-Anforderungen an VPN-Clients. Dabei ist unerheblich, ob die Adressen von einem statischen Pool oder einem DHCP-Server zugewiesen wurden. ISA Server fängt diese Abfragen ab und antwortet anstelle des verbundenen VPN-Clients.Das Subnetz für das VPN-Clientnetzwerk muss nicht vom internen Netzwerk getrennt werden.

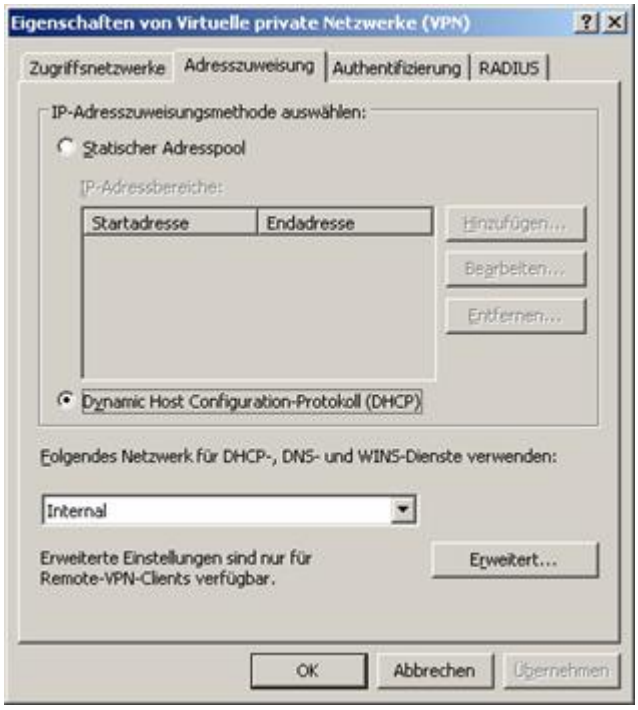
Firewallrichtlinien

Um Remote-VPN-Clients den Zugriff auf Ressourcen des internen Netzwerks zu ermöglichen, muss eine Zugriffsregel erstellt werden, die den entsprechenden Zugriff zulässt. Wenn Sie hinsichtlich der Firewallrichtlinien das VPN-Clientnetzwerk und das interne Netzwerk als identisch betrachten, ist das Erstellen einer Zugriffsregel zu empfehlen, die jeden Datenverkehr vom internen Netzwerk zum VPN-Clientnetzwerk zulässt.

Der ISA Server 2004 erlaubt die so genannte *Stateful VPN Filterung*, dass heißt, Sie können jetzt festlegen, welche Protokolle VPN Clients innerhalb des VPN Tunnels nutzen dürfen. In diesem Beispiel erlauben wir den gesamten Datenverkehr.

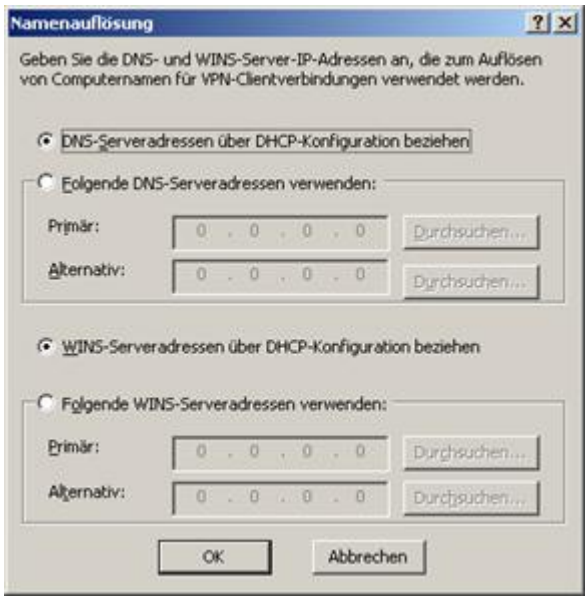
Weitere Eigenschaften der VPN Einrichtung

Klicken Sie mit der rechten Maustaste auf *virtuelle private Netzwerke (VPN)* in der ISA Server Verwaltungskonsole und klicken Sie auf Eigenschaften. Im Reiter *Adresszuweisung* können Sie eine IP-Adresszuweisungsmethode auswählen. Per Default ist DHCP aktiviert. Haben Sie keinen DHCP Server im Einsatz, so wählen Sie *Statischer Adresspol* und geben händisch einen IP-Adressbereich an.



Sie können hier auch festlegen, welches Netzwerkinterface auf dem ISA Server für Dienste wie DHCP, DNS und WINS verwendet werden soll.

Klicken Sie auf *Erweitert* und geben Sie die IP Adressen der DNS- / WINS-Server an.

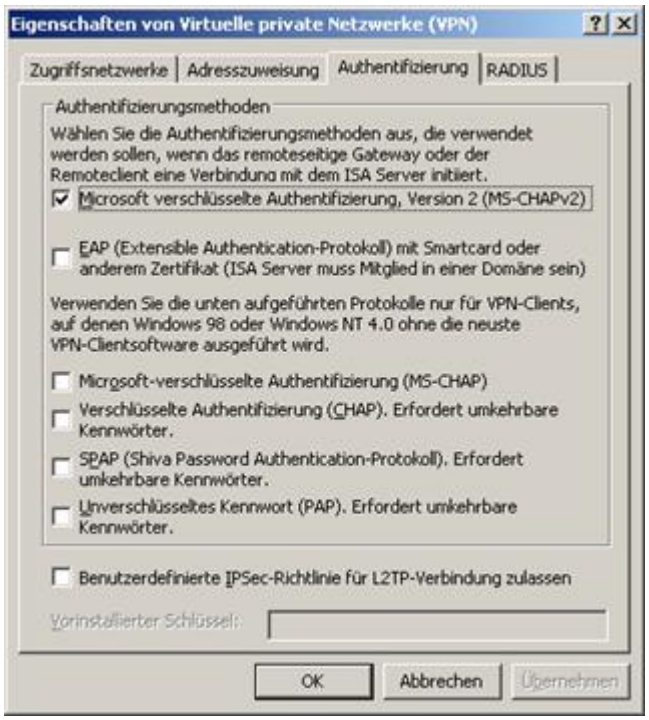


Im Reiter *Authentifizierung* können Sie die Authentifizierungsmethoden festlegen. Per Default ist MS-CHAPv2 aktiviert.

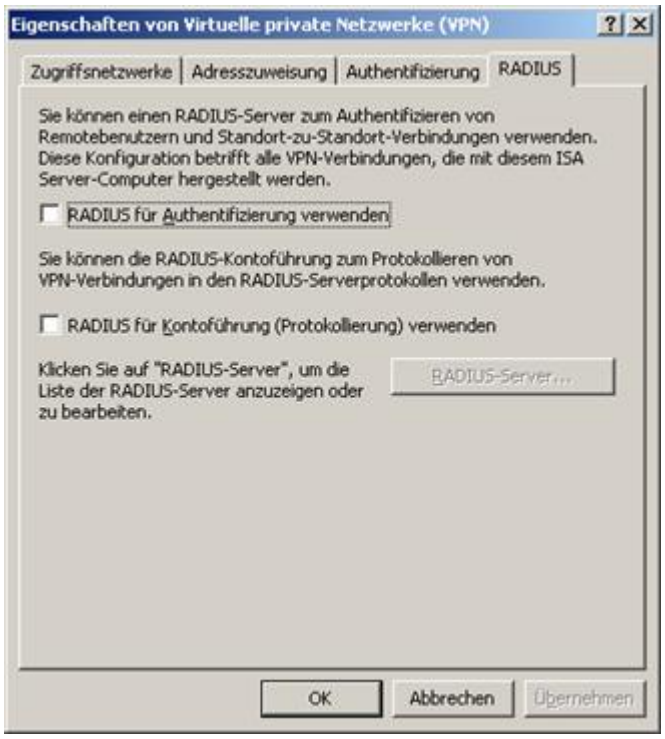
Sie sollten auf die Aktivierung der wesentlich unsicheren Authentifizierungsmethoden

- MS-CHAP / CHAP
- SPAP
- PAP

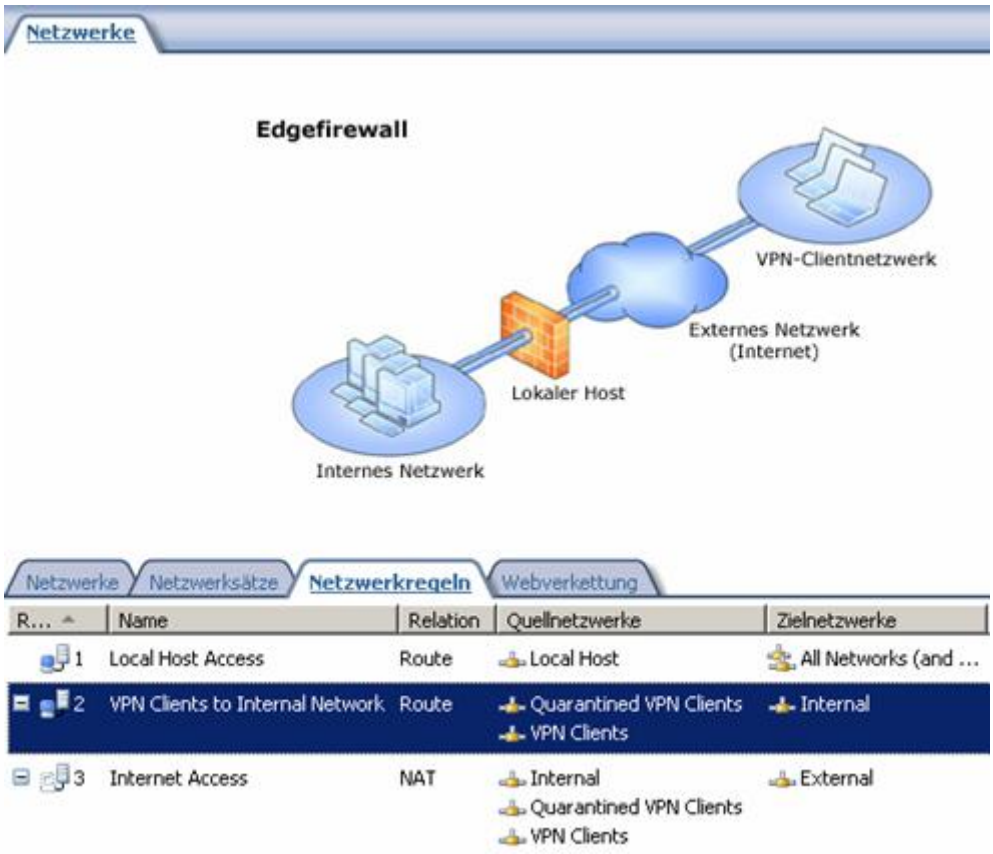
verzichten. In der Regel werden diese Authentifizierungsmethoden nicht benötigt. Für ein Höchstmaß an Sicherheit können Sie auch EAP als Authentifizierungsmethode verwenden. EAP setzt jedoch die Verwendung von Smartcards oder Zertifikaten voraus und erfordert, dass der ISA Server Mitglied einer Domäne ist.



Der Reiter *RADIUS* bietet die Möglichkeit der Authentifizierung über RADIUS.Für mehr Informationen über RADIUS lesen Sie folgenden Artikel

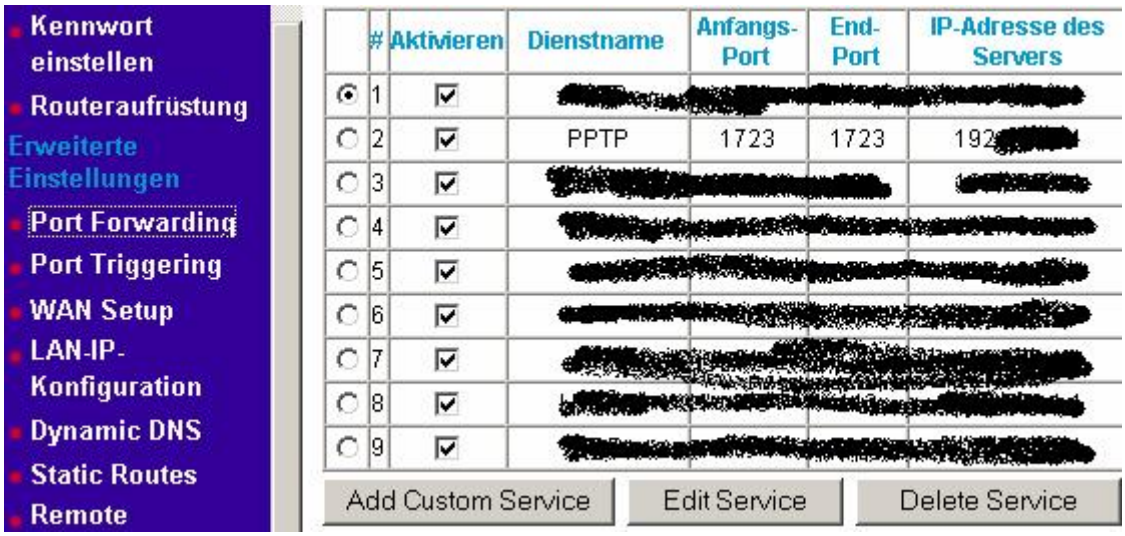


In Schritt 5 überprüfen Sie die erstellte VPN Netzwerkregel. Es wird eine Regel erstellt, welche den *VPN Clients* und *Quarantined VPN Clients* den Zugriff auf das interne Netzwerk zulässt. Die Netzwerkrelation ist ROUTE, das heißt, Datenpakete der VPN Clients werden über den ISA Server in das interne Netzwerk geroutet.



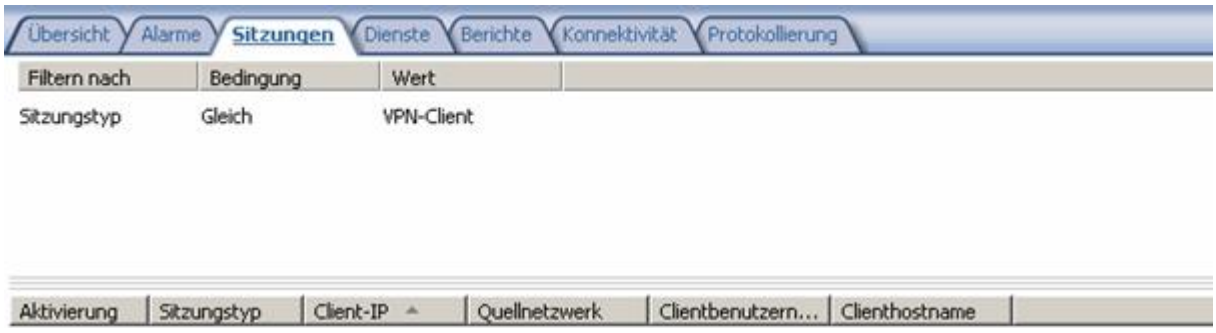
Bei der Installation von ISA Server wird standardmäßig eine Netzwerkregel erstellt, die eine Routingbeziehung zwischen dem internen Netzwerk und dem VPN-Clientnetzwerk definiert. Eine weitere Standardregel wird bei der Installation von ISA Server erstellt. Sie lässt den Zugriff des VPN-Clientnetzwerks auf das externe Netzwerk zu. Um den Datenverkehr zwischen VPN-Clientnetzwerken und anderen Netzwerken zuzulassen, können Sie neue Netzwerkregeln erstellen.

Bemerkung: Normalerweise hängt der ISA Server nicht direkt am Internet, sondern ist über einen Router an das Internet angeschlossen. Sollte das bei Ihnen auch der Fall sein, so müssen Sie am Router ein Portforwarding für PPTP einrichten. Der Router forwarded dann diese Datenpakete an das externe Interface des ISA Servers.Die Einrichtung des Port Forwarding ist von Router zu Router unterschiedlich. Das Beispiel zeigt das Port Forwarding eines SOHO Netgear Routers.



VPN-Verbindungsüberwachung

Sie können VPN-Sitzungen überwachen, indem Sie die Ansicht Sitzungen so filtern, dass nur VPN-Verbindungen angezeigt werden. Konfigurieren Sie den Filter zum Überwachen von VPN-Clients so, dass als Sitzungstyp VPN-Client ausgewählt ist. Konfigurieren Sie zum Überwachen der Verbindungen aus einem Remotestandortnetzwerk den Filter in der Ansicht Sitzungen so, dass für das Quellnetzwerk die Option VPN-Remotestandort ausgewählt ist.



Protokollierung

ISA Server 2004 unterstützt folgende Protokollierungstypen für VPN-Verbindungen:

- Ereignisprotokollierung (Systemprotokoll)
- ISA Server-Protokollierung (MSDE)
- Authentifizierungs- und Kontoführungsprotokollierung auf der Grundlage von RADIUS

Übersicht über die Quarantänesteuerung

ISA Server 2004 bietet ein neues Feature zur sicheren Anbindung von VPN Clients an das lokale Netzwerk – die VPN Quarantine Control.

Die Quarantänesteuerung gewährt Remote VPN Clients, einen Netzwerkzugriff in Stufen. Dieser wird auf einen Quarantänemodus beschränkt, bis der Zugriff auf das Netzwerk zugelassen wird. Sobald sich die Konfiguration des Clientcomputers in Übereinstimmung mit den spezifischen Quarantäneeinschränkungen Ihrer Organisation befindet, wird auf die Verbindung die Standard-VPN-Richtlinie angewendet. Dabei wird der angegebene Quarantänetyp berücksichtigt. In den Quarantäneeinschränkungen kann beispielsweise festgelegt werden, dass während der Verbindung zum Netzwerk Antivirus-Software installiert und aktiviert wird. Obwohl die Quarantänesteuerung keinen Schutz vor Angreifern bietet, können Computerkonfigurationen für autorisierte Benutzer überprüft und ggf. korrigiert werden, bevor diese Benutzer in der Lage sind, auf das Netzwerk zuzugreifen. Darüber hinaus können Sie über einen Zeitraum definieren, nach welchem Zeitraum die Verbindung getrennt wird, wenn der Client die Quarantine Anforderungen nicht erfüllt.

ISA Server 2004 – VPN Quarantine Control

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

Dieser Artikel ist als Ergänzung für den folgenden Artikel zu sehen: VPN mit PPTP und beschreibt die Einrichtung des ISA Server 2004 VPN Quarantine Control Features.

Was ist VPN Quarantine Control?

Bei dem VPN Quarantine Control Feature handelt es sich um ein neues Feature des ISA Server 2004 mit der Möglichkeit, VPN Clients erst dann Zugriff auf interne Netzwerkressourcen zu gewähren, wenn der Client vorher vom Administrator festgelegte Anforderungen erfüllt. Solche vom Administrator festgelegte Anforderungen könnten z. B. sein:

- Einsatz eines aktuellen Virenscanners
- Aktivierte Windows Firewall
- Verwendung der aktuellsten Windows Updates

Bemerkung:

Das VPN Quarantine Control Feature existiert bereits seit der Einführung von Windows 2003.

Bestandteile des VPN Quarantine Control Feature

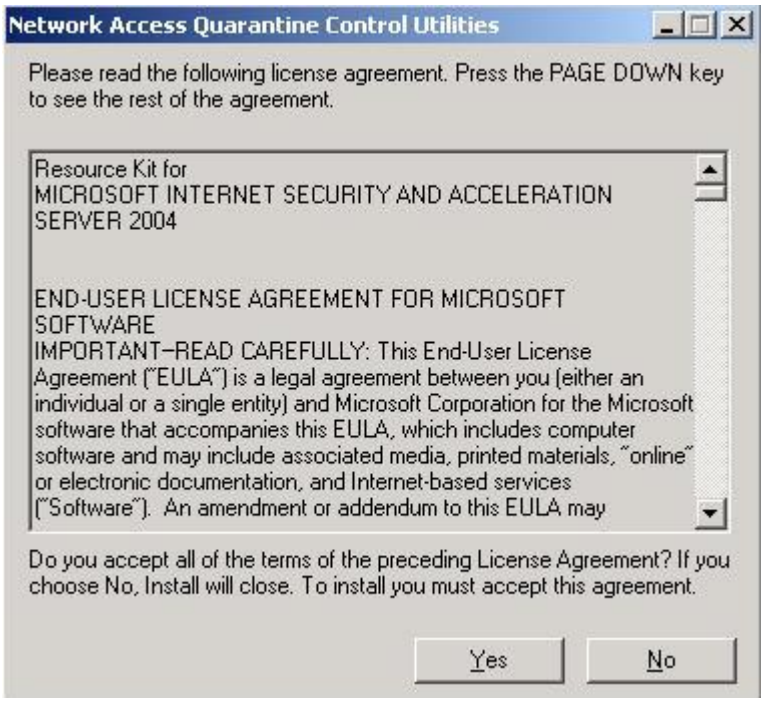
- RQS.EXE – Remote Quarantine Server (Bestandteil des Windows 2003 Resource Kits) auf dem ISA Server 2004
- RQC.EXE – Remote Quarantine Client (Bestandteil des Windows 2003 Resource Kits) auf den VPN Clients
- Connection Manager Administration Profile aus dem Connection Manager Administration Kit (CMAK)
- ConfigureRQSForISA.VBS zur Konfiguration der notwendigen ISA Server 2004 Komponenten

Remote Access Quarantine Control Tool

Die benötigten Quarantine Control Tools sind Bestandteil des Windows 2003 Resource Kits. Sie müssen das Windows 2003 Resource Kit auf dem ISA Server 2004 installieren.

Nach Installation des Windows 2003 Resource Kits müssen Sie ein Update der RQS Komponenten installieren.

Nach dem Download des Tools erfolgt die Installation:



Bemerkung: RQS.EXE ist Bestandteil des Windows 2003 Resource Kits. Es existiert allerdings eine aktuellere Version, welche Sie auf alle Fälle verwenden sollten. Nachdem Sie die Tools installiert haben, führen Sie das Skript ConfigureRQSForISA.vbs aus, um den ISA Server 2004 als RQS Listener Komponente vorzubereiten.

Als nächstes müssen Sie das Skript ConfigureRQSForISA.VBS ausführen.

Dieses Skript führt folgende Aufgaben durch:

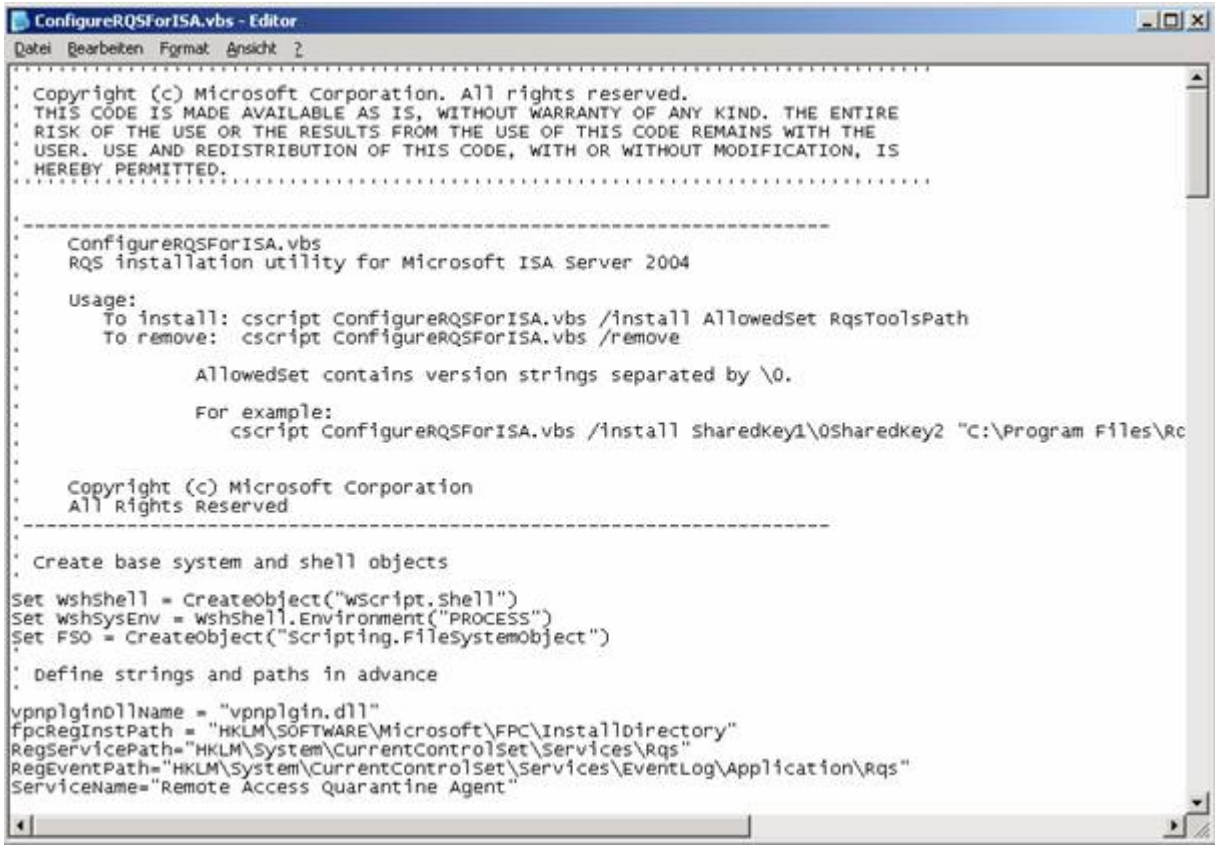
- Erstellt eine RQS Protokolldefinition (TCP Port 7250)
- Erstellt einen RQS Dienst auf dem ISA (Network Quarantine Service (keine Dependencies)
- Erstellt folgenden Registry Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rqs

- Erstellt einen Registry Key, damit RQS Ereignisse korrekt in der Ereignisanzeige dargestellt werden
- Erstellt eine Firewallregel:

- VON: „*Quarantine VPN*“ und „*VPN Client Netzwerke*“
- ZU: „*Local Host Network*“
- PROTOKOLL: RQS
- ERLAUBEN: Alle Benutzer

Der RQS Dienst startet, wenn die Regel aktiviert wird. Der Starttyp ist *Automatisch*

Auszug aus dem Skript:



Wie lautet die Syntax zur Installation des RQS Skriptes für Quarantine Control?

```
cscript ConfigureRQSForISA.vbs /install AllowedSet RqsToolsPath
```

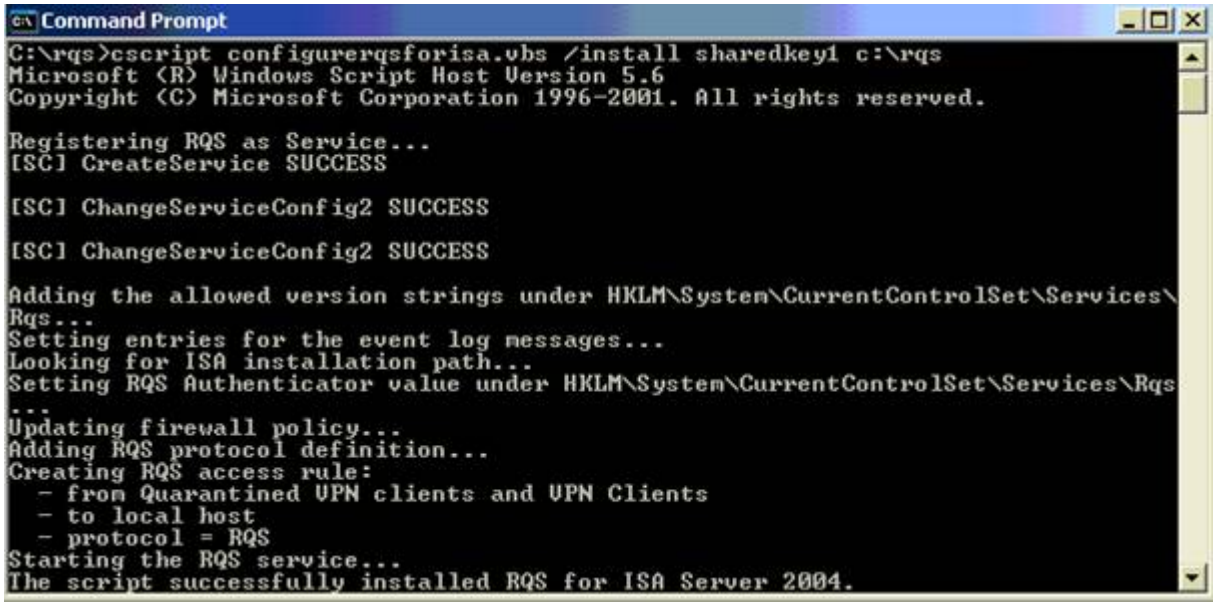
`AllowedSet` ist ein Version String, welcher von der RQC Komponente angegeben werden muss, um sich beim RQS Listener zu identifizieren. Verwenden Sie "\0" um mehrfache Versions Strings zu trennen.

`RqsToolsPath` ist der Pfad zu den RQS Tools ohne Angabe des Dateinamen

Beispiel:

```
cscript ConfigureRQSForISA.vbs /install SharedKey1 "C:\RQS"
```

Bemerkung: Das Skript ConfigureRQSForISA.vbs setzt voraus, dass sich die Dateien SC.EXE und REG.EXE im Windows System Pfad befinden. Das ist bei Windows 2003 der Fall, aber nicht bei Windows 2000.



Erstellter RQS Dienst auf dem ISA Server 2004:

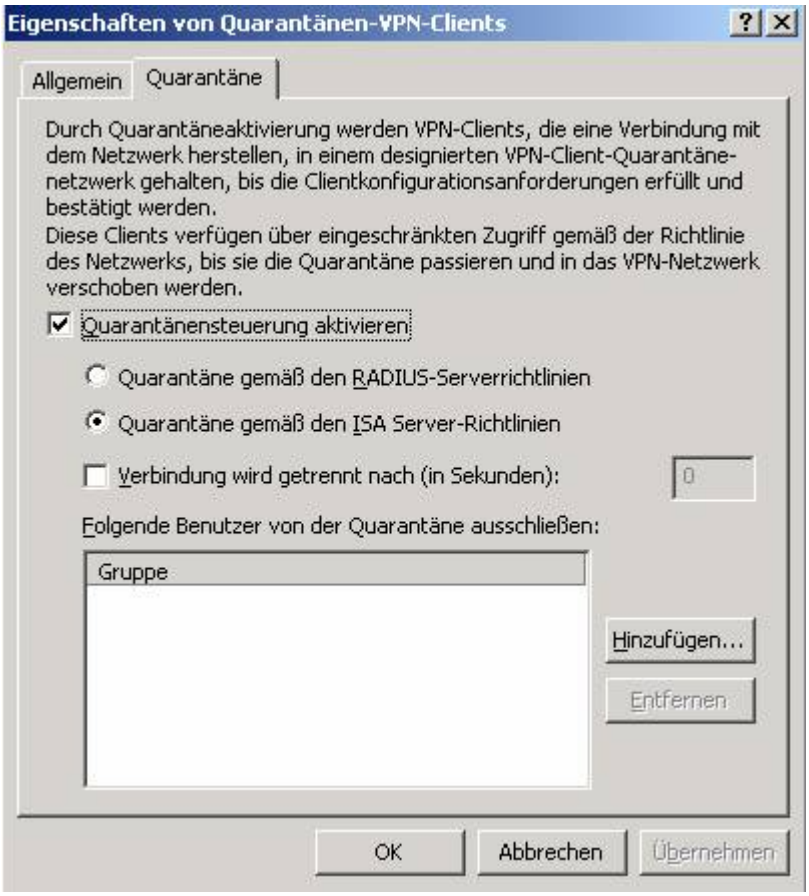
Erstellte Firewall Regel für RQS:

Aktivieren des Quarantine Control Features auf dem ISA Server 2004

Starten Sie die ISA Verwaltungskonsole und navigieren Sie zu Konfiguration – Netzwerke – und wählen im Reiter Netzwerke die Quarantänen-VPN-Clients aus. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontext Menü Eigenschaften aus.

Im Reiter Quarantäne können Sie dann die Quarantänensteuerung aktivieren.

Wählen Sie *Quarantäne gemäß den ISA Server-Richtlinien.*



Bemerkung: Wenn Sie Quarantäne gemäß den RADIUS Server-Richtlinien wählen, muss der ISA Server Mitglied einer Domäne sein. Es sind dann noch weitere Schritte erforderlich.

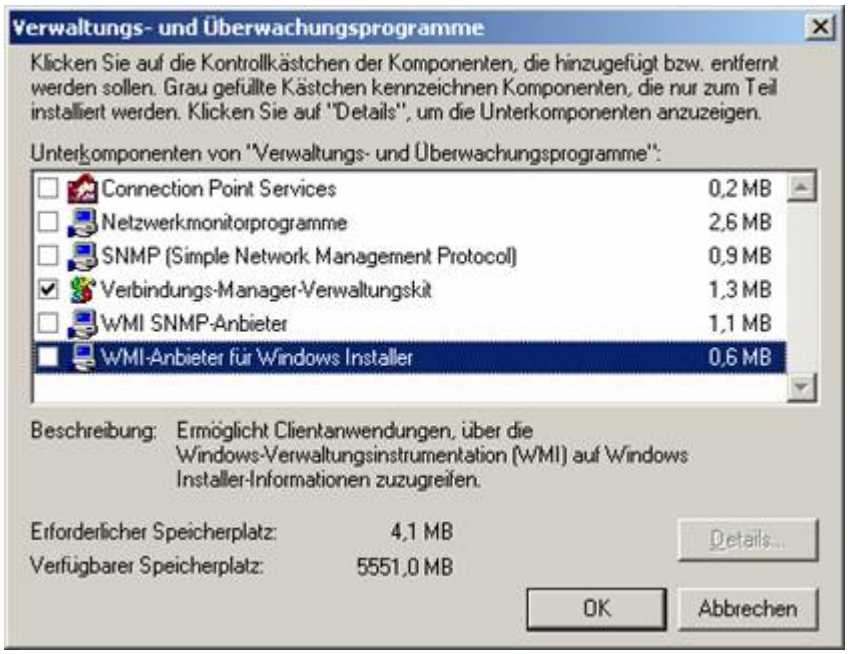
Erstellen einer Firewall Policy für die VPN Clients

Damit die Quarantined VPN Clients Zugriff auf interne Netzwerkressourcen erhalten, müssen Sie eine entsprechende Firewall Policy erstellen. Die Grafik zeigt ein Beispiel:

Details zur Konfiguration von Firewall Policies erhalten Sie hier.

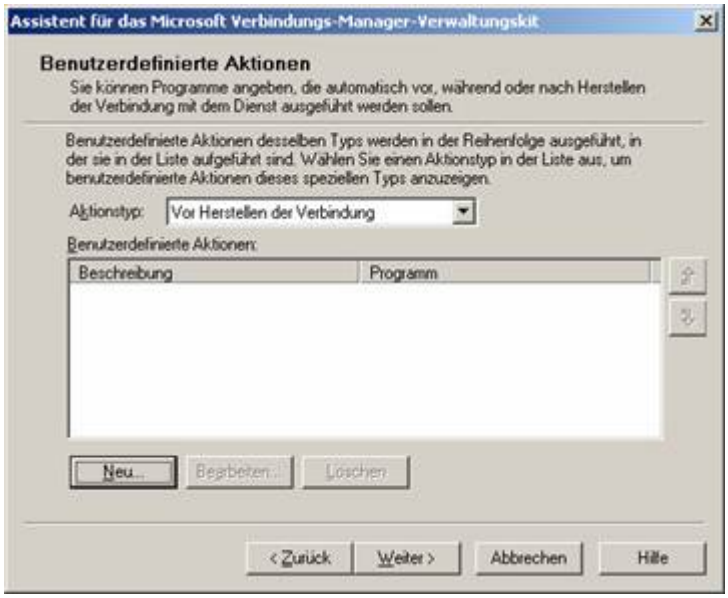
Verbindungs-Manager Profil

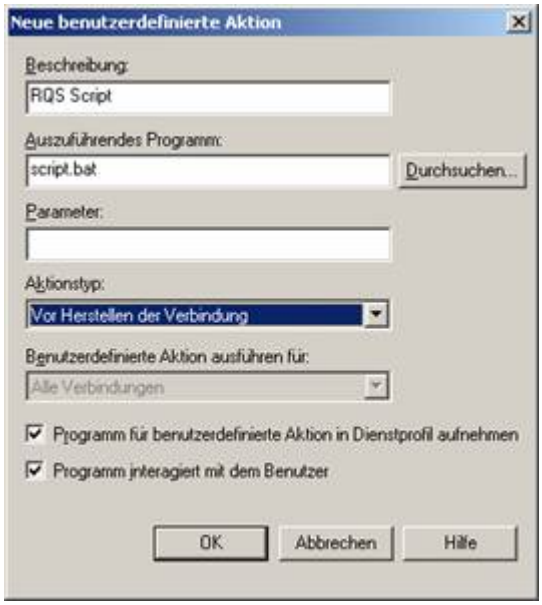
Erstellen Sie mit Hilfe des Verbindungs-Manager Verwaltungskits auf dem ISA Server 2004 ein Connection Manager Profile, mit dessen Hilfe ein VPN Client die Verbindung zum VPN Server aufbauen kann. Bestandteil des CM Profiles ist auch das Quarantine Control Skript.



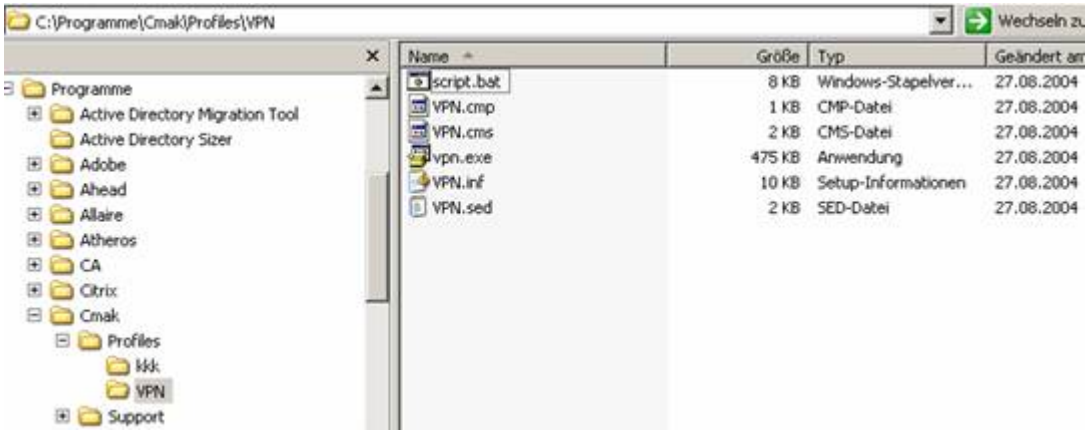
Ich beschreibe in diesem Artikel nicht jeden Schritt zur Konfiguration eines CM Profiles. Für weitere Informationen klicken Sie hier.

Sie müssen das Script (in diesem Beispiel SCRIPT.BAT) als Aktionstyp *Vor Herstellen der Verbindung* ausführen.





CMAK erstellt ein komplettes Profil anhand Ihrer Angaben und packt das ganze in eine .EXE Datei, welche Sie nur noch auf dem VPN Client ausführen müssen.



Nach erfolgter Installation des CMAK Profiles, existiert ein neuer Eintrag in den Netzwerkverbindungen des Clients:

Quarantine Script

Das Quarantine Script kann eine ausführbare Datei (.EXE), Skript (.VBS) oder eine Batchdatei (.CMD oder .BAT) sein.

Nachdem im Script alle Anforderungen des VPN Clients abgefragt worden sind, erfolgt der Aufruf von RQC.EXE mit folgenden Parametern:

```
rqc ConnName TunnelConnName TCPPort Domain UserName
ScriptVersion
```

`ConnName` Der Name der Remote Access Verbindung. Kann mit %DialRasEntry% abgefragt werden!

`TunnelConnName` Der Name der Tunnel Verbindung auf dem Host. Kann mit %TunnelRasEntry% abgefragt werden.

`TCPPort` Die Port Nummer der RQS Komponente. Default = 7250

`Domain` Die Domäne des zu verbindenden Benutzers. Kann mit %Domain%. abgefragt werden.

`UserName` Der Name des Benutzers welcher die Verbindung aufbaut. Kann mit %UserName% abgefragt werden.

`ScriptVersion` Ein text String welcher die Script Version beinhaltet. Sie können alle Textstrings außer /0 verwenden, weil diese vom RQS verwendet werden um mehrfache Strings zu trennen.

Die Erstellung des Quarantine VPN Scriptes ist die schwerste Angelegenheit. Hier hat Microsoft noch einiges erheblich zu verbessern. Die Konkurrenz bietet hier wesentlich komfortablere Konfigurationsmöglichkeiten.

Es ist eine permanente Anpassung des Scriptes notwendig, um es an die sich fast täglich ändernden Sicherheitsbedrohungen anzupassen.

Bemerkung: Mit Windows 2003 SP1 soll es eine GUI zur Konfiguration des Quarantine Control Features geben. Bei meinen bisherigen Test mit der Beta Version von Windows 2003 SP1 konnte ich dieses Programm nicht finden.

Sie können als Einstieg das Beispielscript aus dem Windows 2003 Qurantine Access Control Artikel verwenden. Ich habe das Script in diesem Artikel etwas angepasst. Das Skript kann jedoch nicht für ein reales Quarantine Control Script verwendet werden, zumal es sich bei diesem Beispielsskript nur um ein Gerüst ohne wirkliche Funktion handelt.

Derzeit existieren noch keine frei verfügbaren Beispielskripte auf den Webseiten von Microsoft. Es bleibt zu hoffen, das Microsoft in Zukunft einige Beispielskripte veröffentlicht.

Die Syntax lautet:

```
script.bat %DialRasEntry% %TunnelRasEntry% %Domain% %UserName%
```

Aus `%DialRasEntry%` wird `%1`

Aus `%TunnelRasEntry%` wird `%2`

Aus `%Domain%` wird `%3`

Aus `%UserName%` wird `%4`

```
@echo off
echo    RAS Connection = %1
echo    Tunnel Connection = %2
echo    Domain = %3
echo    User Name = %4
set MYSTATUS=
REM
REM  Netzwerk Poliy Check
REM
REM  Überprüft ob ICF aktiviert ist
REM  Setzt ICFCHECK auf 1 (pass).
REM  Setzt ICFCHECK auf 2 (fail).
REM  Prüft auf installierten Virenchecker
REM  Setzt VIRCHECK auf 1 (pass).
REM  Setzt VIRCHECK auf 2 (fail).
REM  Basierend auf den Ergebnissen wird Rqc.exe ausgeführt
```

```
REM

if "%ICFCHECK%" == "2" goto :TESTFAIL

if "%VIRCHECK%" == "2" goto :TESTFAIL

rqc.exe %1 %2 7250 %3 %4 Version1

REM %1 = %DialRasEntry%

REM %2 = %TunnelRasEntry%

REM 7250 ist der TCP Port auf welchem Rqs.exe einen Listener
setzt

REM %3 = %Domain%

REM %4 = %UserName%

REM Version1 ist die Versionsnummer des Scripts

REM

REM  Statusausgabe

REM

if "%ERRORLEVEL%" == "0" (

      set MYERRMSG=Success!

) else if "%ERRORLEVEL%" == "1" (

      set MYERRMSG=Kein Zugriff möglich. Quarantine Control ist
evtl. deaktiviert

) else if "%ERRORLEVEL%" == "2" (

      set MYERRMSG=Zugriff verweigert. Installieren Sie das
CMAK Profile aus dem Unternehmensnetz.

) else (

      set MYERRMSG=Unbekannter Fehler, der Client bleibt im
Quarantine Mode)

echo %MYERRMSG%

goto :EOF

:TESTFAIL

echo
```

```
echo Der Computer erfüllt nicht die Anforderungen der Security
Policy der Firma IT TRAINING

echo GROTE. Wenden Sie sich an Ihren Administrator um die
Mängel zu beheben und so Zugriff auf

echo Firmenressourcen zu erhalten

:EOF
```

Zusammenfassung:

Welche Schritte werden bei der Verwendung des Quarantine Control Features von ISA 2004 durchgeführt?

- Der Benutzer der Quarantine Remote Access Clients verwendet das installierte Quarantine CM Profil um sich zum ISA 2004 Server zu connecten
- Der Client leitet die Authentifizierungsanfrage an den ISA Server
- Der ISA Server validiert die Authentifizierungsdaten und prüft die Remote Access Policy ob diese die Quarantine Policy matched.
- Die Verbindung wird mit Quarantine Restriktionen akzeptiert und der Client erhält eine IP Adresse und wird im " Quarantined VPN Clients" Netzwerk geparkt
- Der Quarantined Client kann dem ISA Server nur mitteilen, ob das Skript erfolgreich ausgeführt wurde
- Das CM Profile führt das Quarantine Skript als sogenannte „Post Connect" Aktion durch
- Das Quarantine Skript wird ausgeführt und überprüft ob der Remote Access Client den Netzwerk Richtlinien entspricht. Wenn alle Tests bestanden wurden, führt das Skript RQC.EXE aus (mit dem Text String, welcher im CM Profil angegeben wurde)
- RQC.EXE sendet eine Notifikation an den ISA Server das das Skript erfolgreich ausgeführt wurde.
- Die Notifikation wird von der RQS Listener Komponente empfangen (es wird nur Traffic über den RQS Port 7250 erlaubt)
- Die Listener Komponente überprüft den Skript Version String in der Notification Message und schickt eine Bestätigung zurück.
- Wenn das Skript validiert wurde, ruft die Listener Komponente die MprAdminConnectionRemoveQuarantine() API auf, welche den ISA Server dazu veranlasst, den Client aus dem „Quarantined VPN Clients network" in das „VPN Clients Network" verschiebt.
- Die Listener Komponente erstellt ein Ereignis in die Ereignisanzeige (System)

Clientkonfiguration für PPTP-VPN-Verbindungen mit PocketPC 2002

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2000
- Microsoft ISA Server 2004
- Clientbetriebssystem: Microsoft PocketPC 2002

So ein PocketPC ist eine sehr nette und nützliche Sache. Je nach Ausstattung und Konfiguration nahezu überall Zugriff auf das Internet und ggfs. auf das Firmennetzwerk samt Synchronisation mit Outlook/Exchange. Gerade für Administratoren oder Consultants ist der für PocketPC verfügbare Remotedesktopclient (Terminaldiensteclient) sicherlich interessant. Eine bestehende IP-Verbindung vorausgesetzt (entweder per Bluetooth - Handy - GPRS oder per WLAN) kann man per RDP auf einen Server zugreifen und ihn fernsteuern oder Konfigurationen vornehmen. Allerdings ist das kleine Display gewöhnungsbedürftig.

Was allerdings, wenn der Terminalserver, der Exchange- oder Mailserver nicht öffentlich im Internet verfügbar sind, sondern durch einen ISA Server geschützt werden? In diesem Fall bietet es sich an, vom PocketPC aus eine VPN-Verbindung zum ISA aufzubauen. Dann ist man wie mit einem "normalen" Windows Client mit einer LAN-internen IP Adresse ausgestattet und kann auf sämtliche Ressourcen zugreifen. Das ist vom Prinzip her genauso einfach wie bei einem Windows 2000/XP Client.

Hinweis: Wenn Sie Exchange Server 2003 einsetzen können Sie mittels ActiveServerSync den PocketPC mit Exchange ohne ein VPN synchronisieren. Sie müssen dazu lediglich eine Webserververöffentlichung für diesen Dienst erstellen.

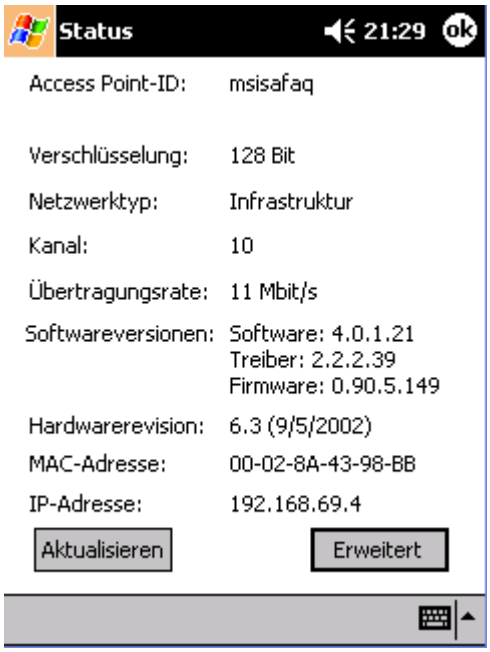
Sehen wir uns das Setup Schritt für Schritt an:

1. Herstellen einer Internetverbindung

Bevor eine VPN-Verbindung zum FirmenLAN hergestellt werden kann muss eine Internetverbindung bestehen. Na gut, es gibt auch noch die Möglichkeit, sich z.B. per HSCSD direkt in den RAS-Server einzuwählen. Im folgenden wird jedoch der gebräuchlichere Weg über eine Internetverbindung beschrieben.

WLAN

WLAN ist die bandbreitenbeste Verbindung für einen PocketPC. Je nach Gerät muss natürlich zuerst eine WLAN-Karte eingesetzt und installiert werden. Das Beispiel hier verwendet einen HP iPAQ 5450 mit integriertem Bluetooth und WLAN.

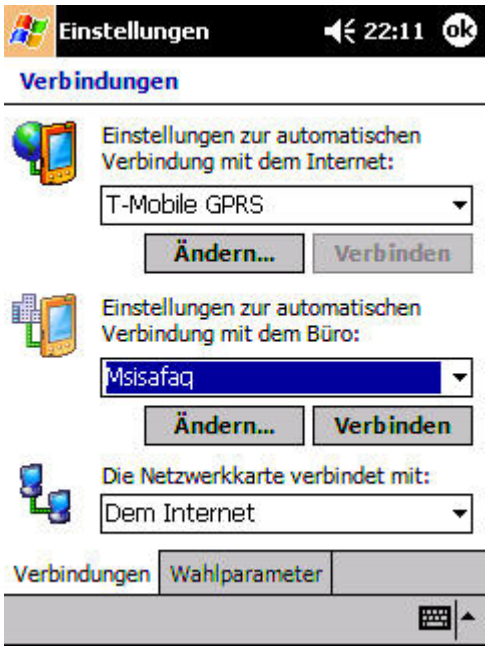


Bluetooth

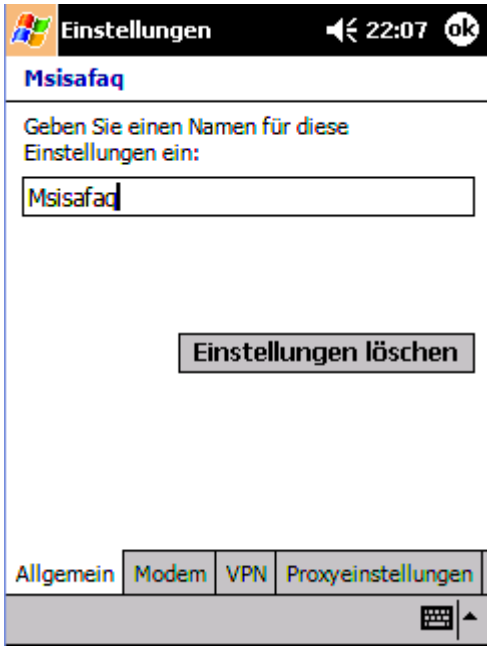
Nicht überall ist natürlich ein WLAN-HotSpot verfügbar. Wer ein bluetoothfähiges Mobiltelefon sein Eigen nennt, kann damit eine GPRS-Verbindung zum Internet aufbauen. Mittlerweile dürfte jeder Netzanbieter/Provider diesen Zugang zu erträglichen Kosten anbieten. Eine gute Anleitung zum Verbindungsaufbau über GPRS gibt es z.B. auf der Seite http://www.pocket-expert.de/. Auf dieser Website finden Sie sehr viele nützliche Tipps rund um den PocketPC.

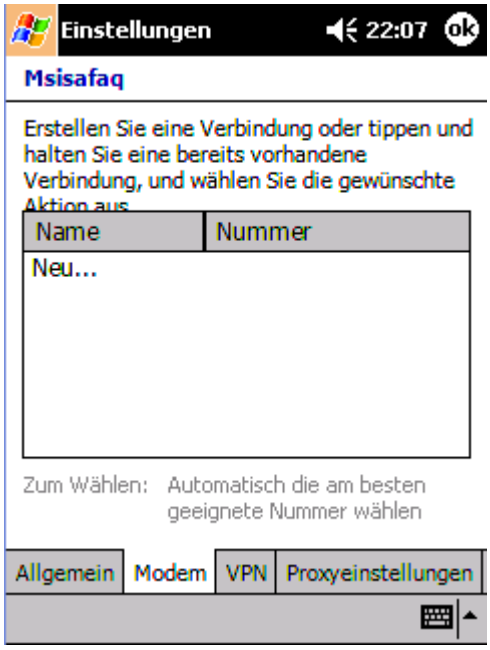
2. Einrichten einer neuen VPN-Verbindung

Über Start -> Einstellungen -> Verbindungen -> Verbindungen kommt man zu folgendem Screen:

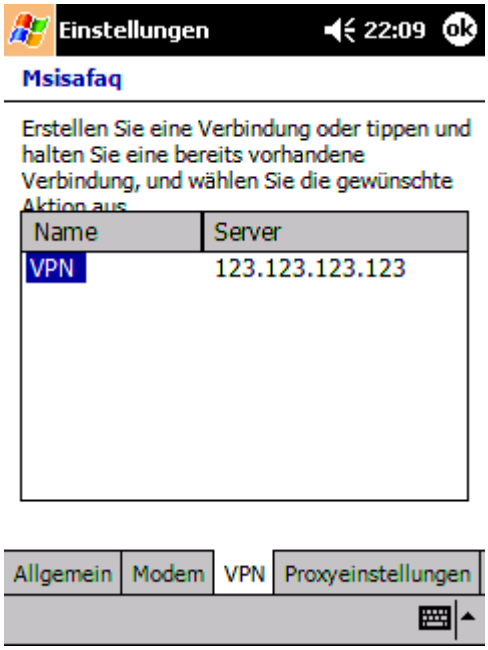


Sehen wir uns die Einstellungen von "Msisafaq" näher an:

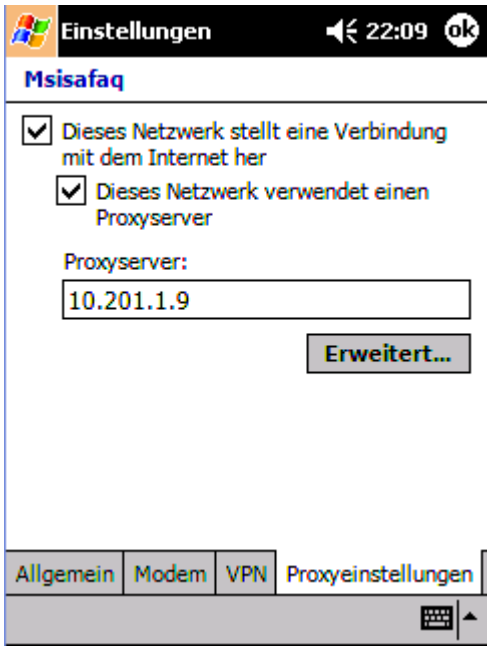




Der Bereich "Modem" kann/soll unverändert gelassen werden.



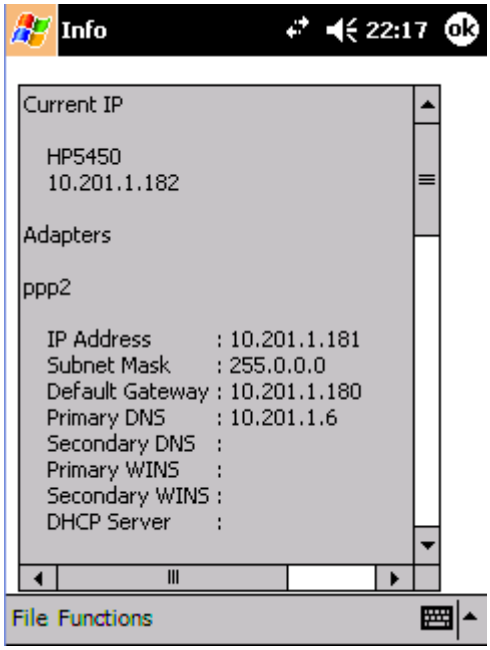
Durch Doppelklick auf den blau hinterlegten Eintrag "VPN" (Name frei wählbar) kommt man zur Eingabemaske der IP-Adresse oder des FQDN für den VPN-Server.



Wenn bei aktiver VPN-Verbindung auch über diese der HTTP-Traffic abgewickelt werden soll, an dieser Stelle die IP des internen ISA Servers eintragen.

Das war die Konfiguration des PocketPC für VPN. Beachten Sie, dass derzeit nur PPTP möglich ist.

Nachdem man mit dem FirmenLAN verbunden ist, bekommt man im Regelfall per DHCP oder RAS-IP-Pool (weitere Infos hier) eine interne IP Adresse zugewiesen. Dies kann man z.B. mit den *vxUtils* ansehen:



Ein weiteres sehr nützliches Tool ist *Pocket Hosts* von Marc Zimmermann. Damit hat man die Möglichkeit, hosts Einträge wie am PC zu setzen.

Clientkonfiguration für PPTP-VPN-Verbindungen mit Windows 2000/XP

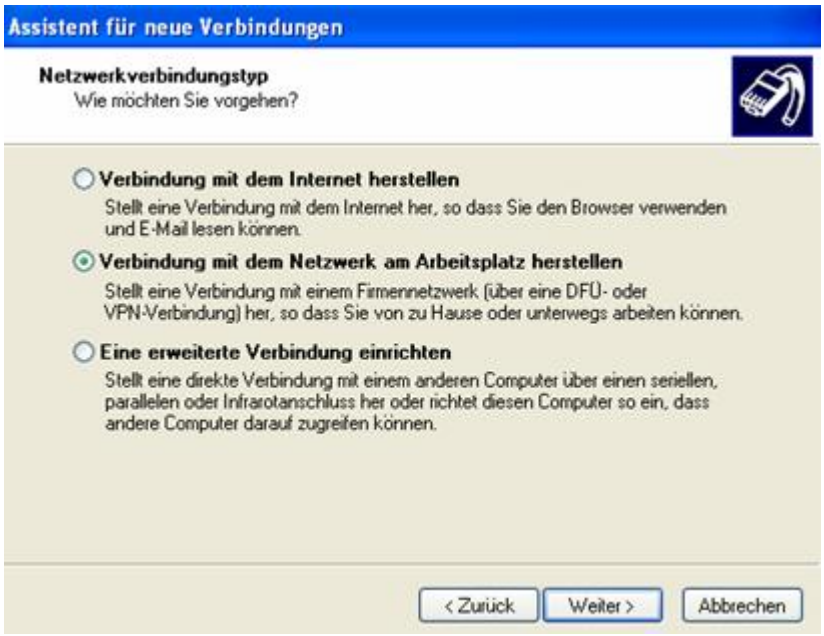
Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2000
- Microsoft ISA Server 2004
- Clientbetriebssystem: Microsoft Windows 2000 / XP

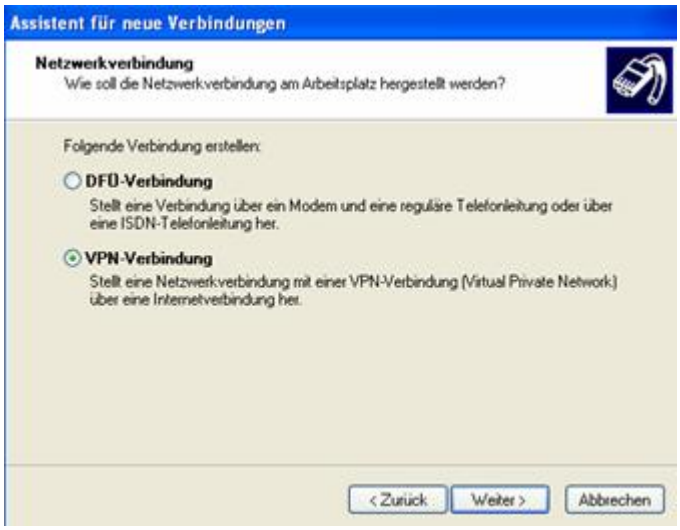
Im Artikel VPN mit PPTP wurde beschrieben, wie der ISA Server als VPN Server konfiguriert wird. Dieser Artikel beschreibt die notwendige Clientkonfiguration am Beispiel eines Windows XP Client mit SP2.

Zur Einrichtung einer neuen VPN Verbindung klicken Sie auf *Start – Systemsteuerung – Netzwerkverbindungen* – und unter *Netzwerkaufgaben* auf *Neue Verbindung erstellen.*

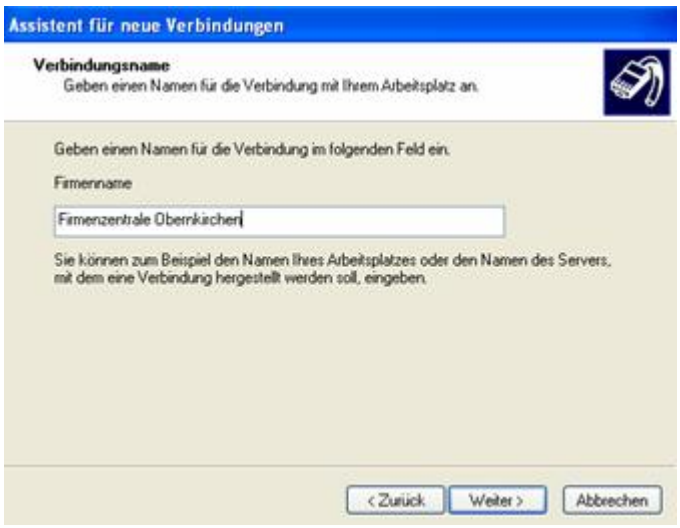
Als Netzwerkverbindungstyp wählen Sie *Verbindung mit dem Netzwerk am Arbeitsplatz herstellen*.



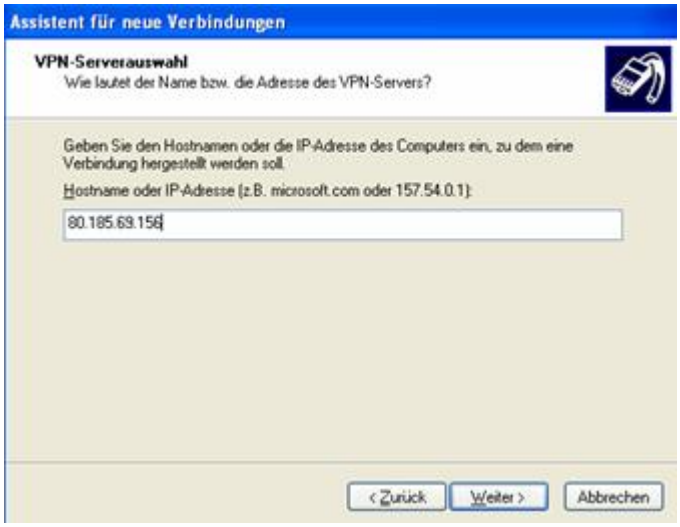
Wählen Sie *VPN-Verbindung*



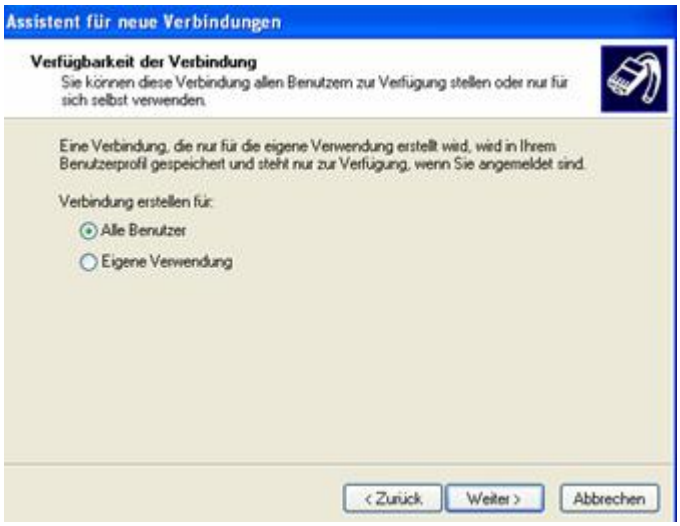
Vergeben Sie einen Namen für die VPN Verbindung.



Geben Sie hier den Hostnamen oder die IP Adresse des VPN-Servers (ISA 2004) an. In diesem Beispiel verwende ich eine vom ISP dynamisch zugewiesene IP Adresse und nicht den Hostnamen.

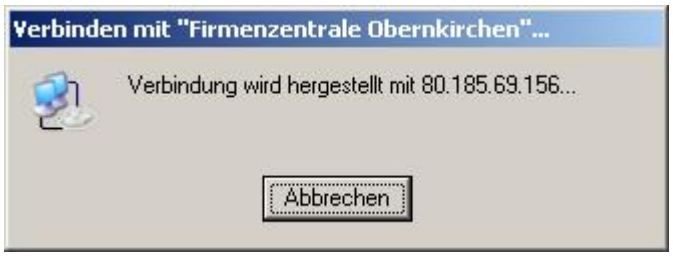


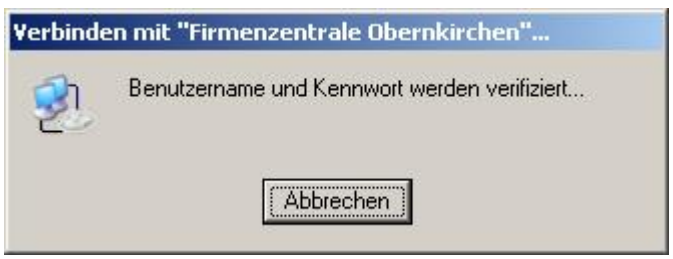
Legen Sie jetzt noch fest, für welche Benutzer diese Verbindung nutzbar ist.



Der Assistent hat die Verbindung konfiguriert.

Sie können jetzt eine Verbindung herstellen.





Nach erfolgreicher Authentifizierung ist die Verbindung hergestellt.

Status von Firmenzentrale Obernkirchen
Allgemein
Details
Eigenschaft
Wert
Gerätename
WAN-Miniport (PPTP)
Gerätetyp
vpn
Servertyp
PPP
Übertragungen
TCP/IP
Authentifizierung
MS CHAP V2
Verschlüsselung
MPPE 128
Komprimierung
(keine)
PPP-Multilinkframing
Inaktiv
Server-IP-Adresse
169.254.48.100
Client-IP-Adresse
169.254.71.45
Schließen

Einrichten einer Internetanbindung über eine DFÜ Verbindung

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

Dieser Artikel beschreibt die Einrichtung einer ISDN DFÜ Verbindung zur Verwendung als Einwahlinterface für einen Microsoft ISA Server 2004.

Nicht jede Firma ist im Besitz einer Standleitung oder DSL Flatrate Verbindung mit einem Router, um mit dem ISA Server 2004 eine Verbindung zum Internet herzustellen. Gerade in kleineren Firmen steht evtl. nur eine ISDN Verbindung zur Verfügung.

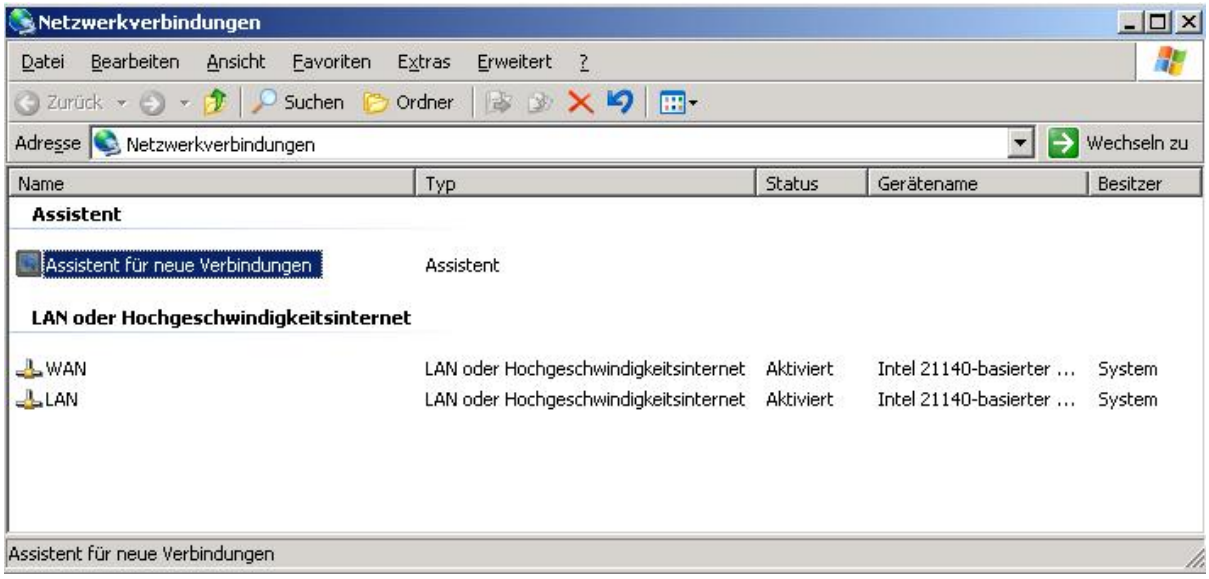
ISA Server 2004 unterstützt die Verbindung mit dem Internet über eine DFÜ Verbindung.

In diesem Beispiel verwenden wir den Internet Call-by-Call Anbieter Callisa und eine AVM Fritz Card. Die Installation und Konfiguration der ISDN Karte wird in diesem Artikel nicht beschrieben und vorausgesetzt.

Bemerkung:

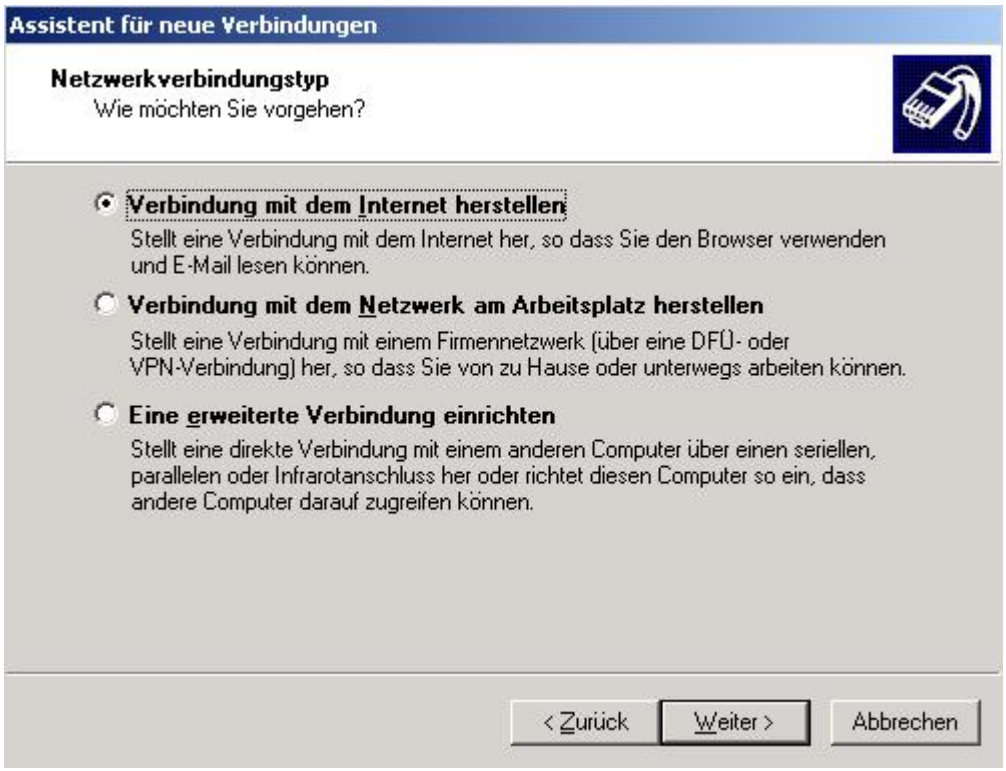
In der Regel ist ein Internet Call-by-Call Anbieter auf Dauer zu kostenintensiv, weil der ISA Server bei jedem ausgehenden Datenpaket eine DFÜ Verbindung aufbaut. Sollten Sie mit einer Einwahlverbindung arbeiten müssen, so empfehle ich die Wahl einer ISDN Flatrate oder eines Volumentarifs. Ein Zeittarif kann schnell zu hohen Kosten führen.

Im ersten Schritt müssen Sie die DFÜ Verbindung konfigurieren. Starten Sie dazu den ***Assistent für neue Verbindungen*** in dem Sie auf ***Start - Verbinden mit - Alle Verbindungen anzeigen*** klicken.

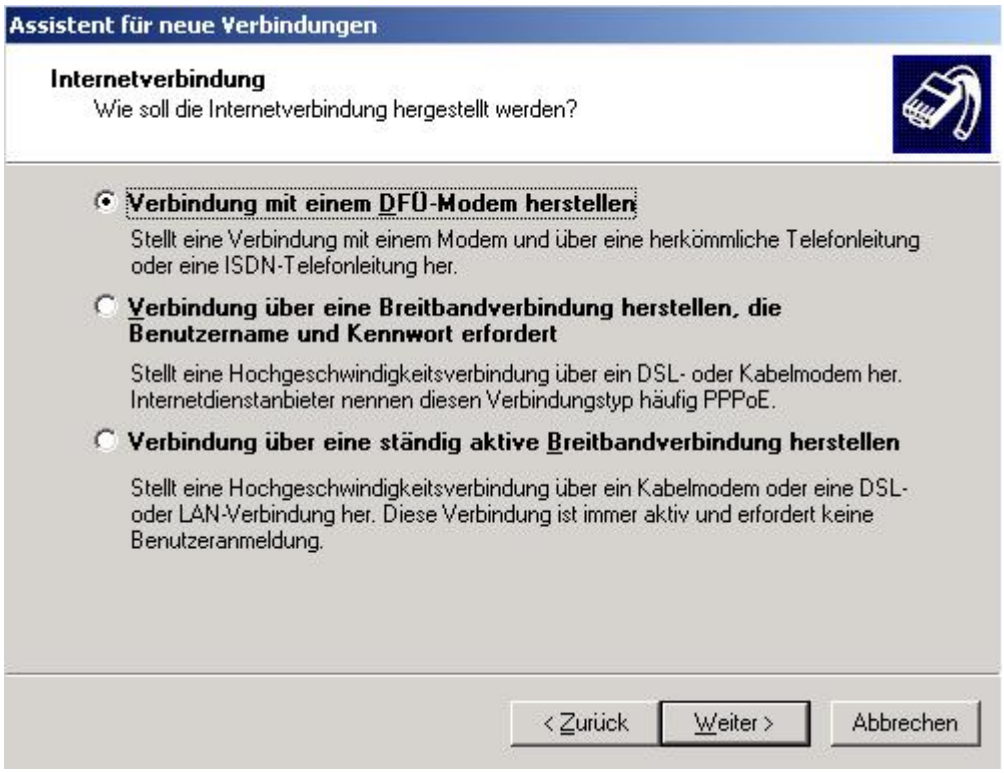


Klicken Sie auf ***Weiter***

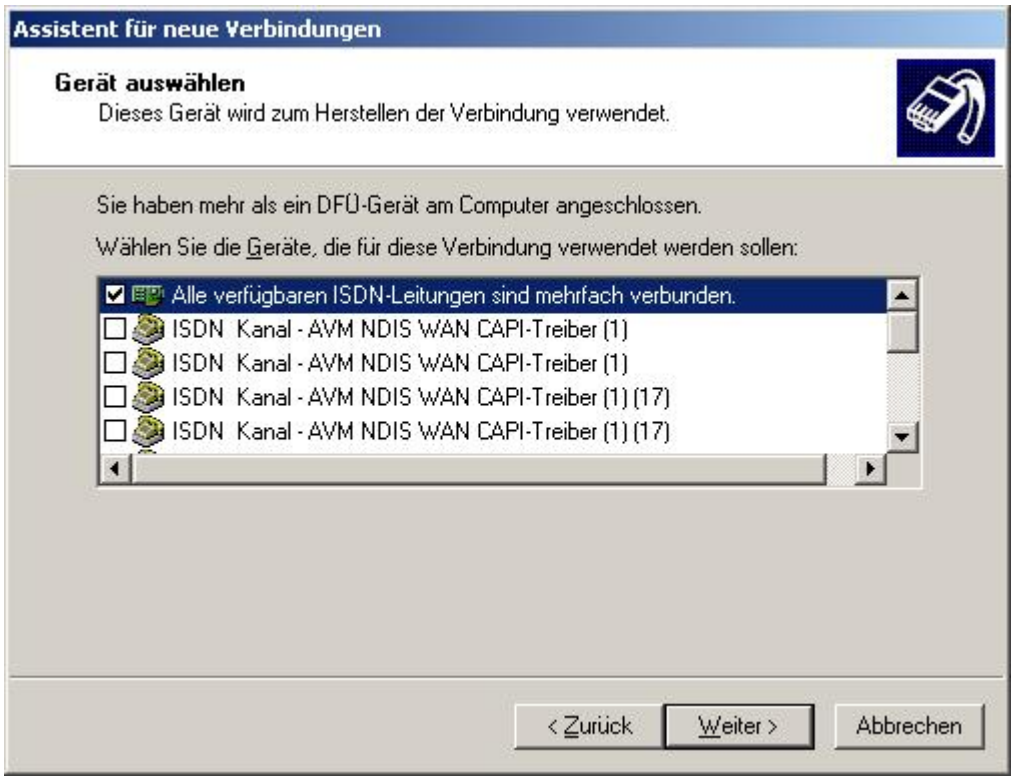
Wählen Sie ***Verbindung mit dem Internet herstellen.***



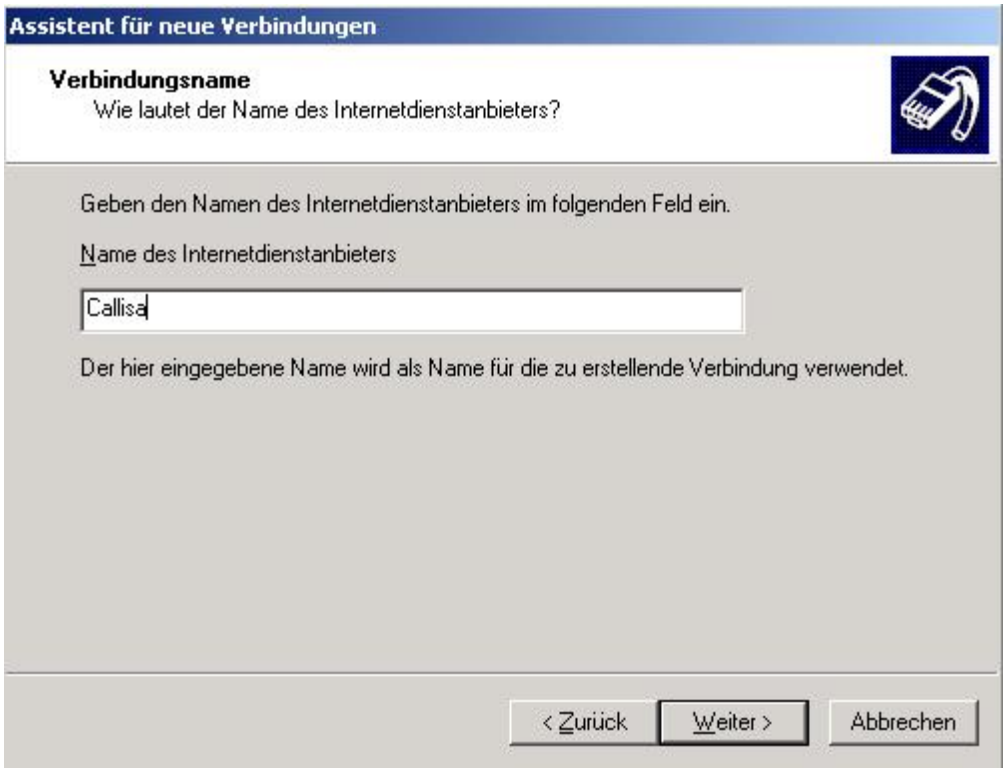
Wählen Sie ***Verbindung mit einem DFÜ-Modem herstellen.***



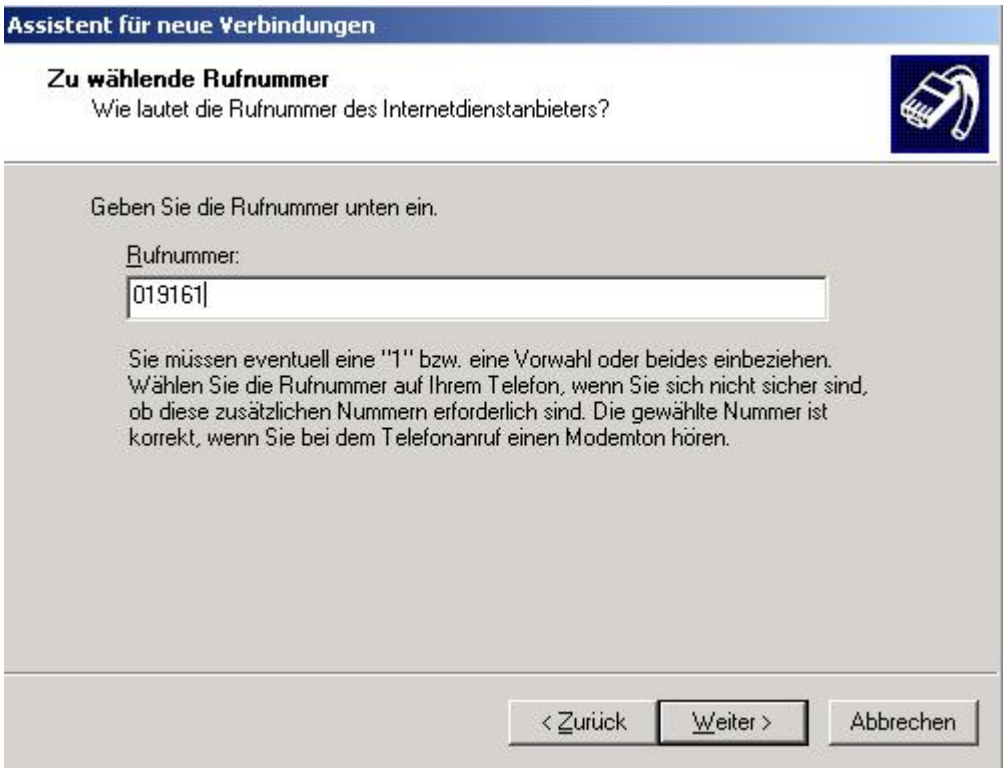
Wählen Sie das Gerät zum Herstellen der Verbindung aus.



Geben Sie einen Namen für die Verbindung an.



Geben Sie die Rufnummer des Internetdienstanbieters an.



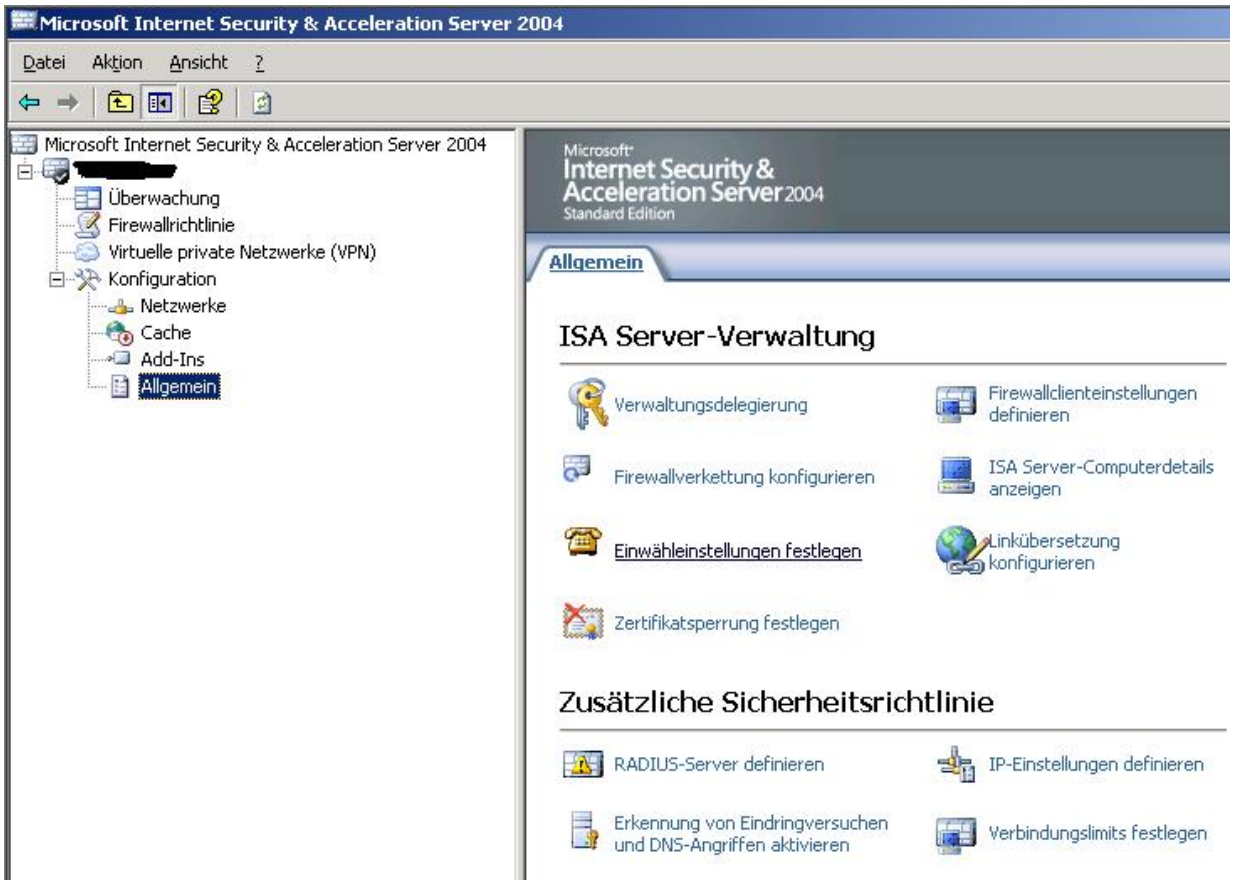
Für wen soll die Verbindung zur Verfügung stehen? Wir wählen in diesem Beispiel ***Alle Benutzer.***

Geben Sie jetzt die Internetkontoinformationen für das Herstellen der Verbindung zum Internet Provider an. Die Daten erfahren Sie bei Ihrem Internetanbieter. Die beiden Haken können Sie gesetzt lassen.

Der Assistent hat alle Informationen erhalten. Sie können den Assistenten mit einem Mausklick auf ***Fertig stellen*** beenden.

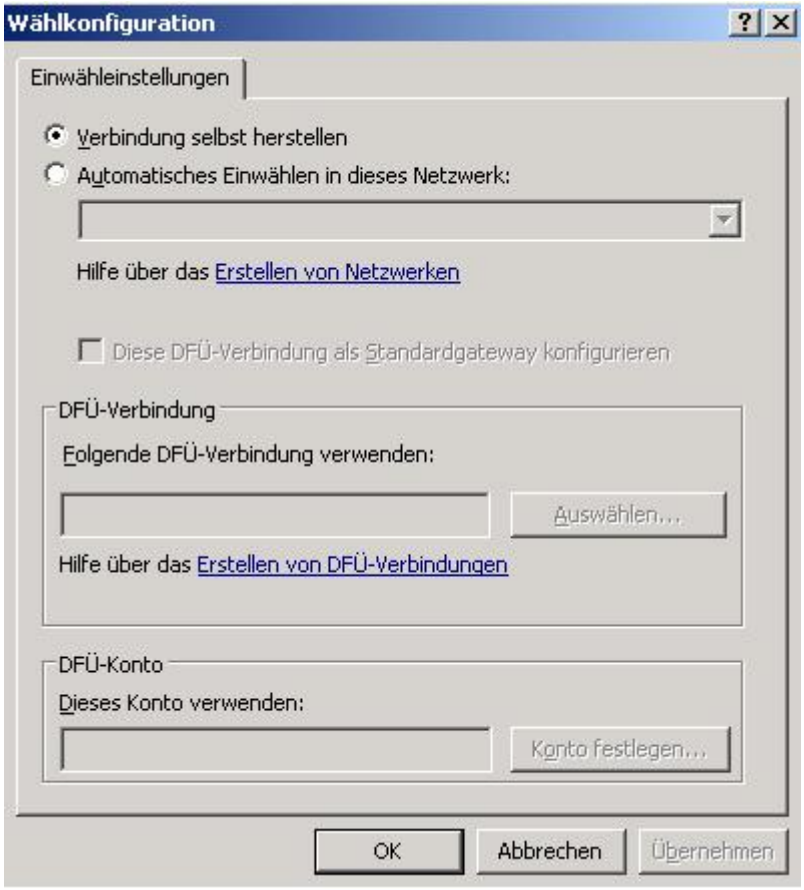
Die DFÜ Verbindung ist jetzt konfiguriert. Im nächsten Schritt müssen Sie jetzt den ISA Server 2004 zur automatischen Einwahl konfigurieren.

Starten Sie dazu die ISA Server 2004 Verwaltungskonsole und navigieren Sie zu dem Container ***Allgemein*** unterhalb des Container ***Konfiguration.***



Klicken Sie auf ***Einwähleinstellungen festlegen.***

Die DFÜ-Verbindung beinhaltet DFÜ-Eigenschaften wie den Internetdienstanbieter (ISP), die Einwahlnummer und das Modem.
Nach der Auswahl einer DFÜ-Verbindung müssen die vom Internetdienstanbieter (ISP) angeforderten DFÜ-Kontoinformationen angegeben werden. Es müssen dieselben Kontoinformationen eingegeben werden wie beim Erstellen der DFÜ-Verbindung. Die DFÜ-Kontoinformationen werden von ISA Server verwendet, wenn eine Verbindung zum Internetdienstanbieter hergestellt wird.



Bemerkung:

Vergewissern Sie sich, dass auf den internen Netzwerkadaptern des ISA Server-Computers kein Standardgateway konfiguriert ist.

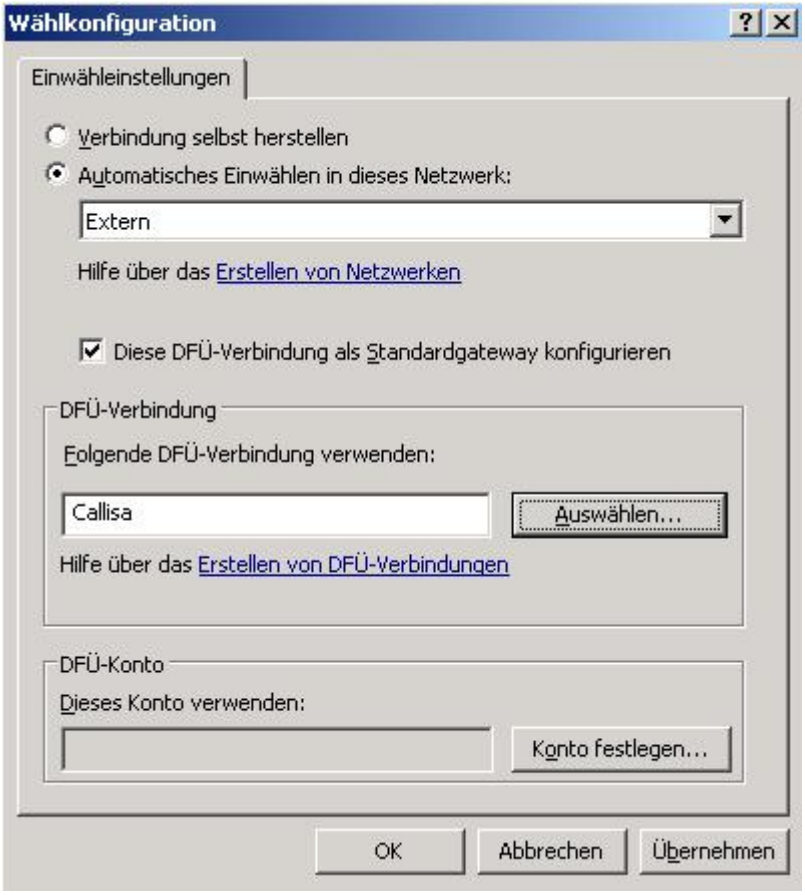
Klicken Sie auf ***Automatisches Einwählen in dieses Netzwerk*** und wählen Sie das ***externe*** Netzwerkinterface (das Externe Netzwerkinterface hat in diesem Beispiel den Namen Extern).

Bemerkung:

Ich empfehle Ihnen, nach der Installation des Windows 2003 Servers die Netzwerkkarten entsprechend deren Verwendung umzubenennen, damit Sie bei der späteren Verwaltung des ISA Servers nicht die Übersicht verlieren. Das interne Netzwerkinterface können Sie z. B. INTERN nennen und das externe Interface EXTERN.

Diese DFÜ-Verbindung als Standardgateway konfigurieren

Legt fest, dass bei der Verwendung dieser DFÜ-Verbindung auch das externe Netzwerk über den DFÜ-Adapter erreichbar ist.



Automatisches Einwählen in dieses Netzwerk.

Das automatische Einwählen wird für ein bestimmtes Netzwerk konfiguriert. Wenn ISA Server 2004 eine Anforderung für das ausgewählte Netzwerk erhält, wird die DFÜ-Verbindung verwendet, die für dieses Netzwerk konfiguriert wurde.
Das automatische Einwählen kann nur für ein Netzwerk verwendet werden.
Wenn das automatische Einwählen für die Verbindung ins Internet verwendet wird, sollten Sie als automatische DFÜ-Verbindung das externe Netzwerk auswählen.

DFÜ-Verbindung

Klicken Sie auf ***Auswählen*** und wählen Sie die zuvor konfigurierte DFÜ-Verbindung aus.

DFÜ-Konto

Dient zum Eingeben des Benutzernamens eines zum Zugriff auf die DFÜ-Verbindung berechtigten Benutzers. Klicken Sie auf ***Konto festlegen***, um ein Benutzerkonto auszuwählen, das mit der DFÜ-Verbindung verwendet wird. Verwenden Sie hierbei nicht ein Windows Benutzerkonto, sondern die Verbindungsdaten für die Verbindung zum Internetdienstanbieter.

Die Konfiguration ist beendet. Sie können jetzt überprüfen, ob der ISA Server automatisch eine Verbindung mit dem konfigurierten Internetdienstanbieter herstellt, sobald der ISA Server 2004 Anfragen aus dem internen Netzwerk oder vom ISA Server selbst erhält.

SMTP/POP3 ausgehend nicht möglich

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

In der Newsgroup und im Rahmen meiner täglichen Arbeit wird häufig gefragt, warum ein Mailclient nach der ISA Installation keine Mails mehr senden bzw. empfangen kann. Was dafür am ISA Server zu konfigurieren ist habe ich im Artikel Mailzugriff ausführlich beschrieben.

An dieser Stelle möchte ich Möglichkeiten aufzeigen, wie ein Konfigurationsfehler gesucht und ggfs. gefunden werden kann.

Problem: Interner Mailclient (z.B. Outlook) kann keine Mails versenden und empfangen

Lösungsvorschläge:

1. Überprüfen, ob eine Firewallrichtlinie für SMTP- und POP3-Verkehr erstellt ist und ob ggfs. Zugriffs-Einschränkungen existieren (vgl. den o.g. msisafaq-Artikel)
2. Überprüfen, ob der ISA Server eine Verbindung zum Internet hat (speziell bei Anbindungen über DFÜ)
3. Sicherstellen, dass der interne Client ein SecureNAT-Client oder ein Firewall-Client ist.
4. Mittels des DOS-Kommandos `telnet` einen Verbindungsaufbau testen:

```
telnet mail.msisafaq.de 25 Bitte diesen Befehl in einer
Kommandozeile eingeben. Verwenden Sie statt mail.msisafaq.de den
Mailserver Ihres Providers; der msisafaq-Mailserver ist in dieser
Form von aussen nicht erreichbar. Port 25 ist für SMTP zuständig,
testen Sie ggfs. auch Port 110 für POP3.

220 mail.msisafaq.de msisafaq ESMTP Mailserver Version
7.0.0.2002 Sat, 13 Jul 2002 20:34:52 +0200 Wenn eine
Verbindung zum Mailserver hergestellt werden kann erhalten Sie
abhängig vom Zielmailserver eine ähnliche Meldung.
quit Beenden Sie die Verbindung zum Mailserver; weitere Tests sind
nicht notwendig.
221 2.0.0 mail.msisafaq.de Service closing transmission
channel
```

5. Bekommen Sie keine Verbindung UND haben Sie die ersten drei Punkte kontrolliert, verwenden Sie statt dem FQDN die IP-Adresse des Mailservers.
6. Hat der Verbindungsaufbau geklappt? Wenn ja, gehen Sie zu 8.
7. Verwenden Sie testweise einen anderen Mailserver
8. Sicherstellen, dass die Namensauflösung per DNS funktioniert

Interessante Knowledge Base Artikel

Auswahl einiger Artikel aus der Microsoft Knowledge Base zu häufigen Problemen und Themen rund um den ISA Server 2004:

- 890306 - You receive event ID 14192, and the Internet Security and Acceleration Server (ISA) 2004 Control service does not start
- 888642 - Programs and services on a Firewall Client computer may not be able to access remote resources in ISA Server 2004
- 888647 - Users are repeatedly prompted for credentials and authentication is not successful when a downstream computer that is running ISA Server 2004 uses Integrated Windows authentication to authenticate to an upstream computer that is running ISA Server 2004
- 887000 - You receive a "The remote procedure call failed" error message and RPC route publishing is not permitted in ISA Server 2004
- 888927 - Host headers and URLs are considered to be encoded by UTF8 encoding in Internet Security and Acceleration Server 2004
- 888652 - Some 16-bit files may be installed when you install ISA Server 2004
- 888646 - Changes that you make by using the Firewall Client are not applied to all users
- 885351 - You cannot browse Web servers on a remote site when you use IPsec tunnels to connect sites on a Windows Server 2003-based computer that is running Internet Security and Acceleration Server 2004
- 888709 - When to use the ISA Server 2004 SMTP filter and Message Screener
- 888715 - Export, import, and backup functionality in Internet Security and Acceleration Server 2004
- 888644 - You may not be able to connect to a Proxy Server 2.0 server or to an ISA 2004 server or ISA 2000 server that requires a UDP-only control channel by using an ISA Server 2004 Firewall client
- 888708 - List of common scenarios that the "VPN Roaming Clients and Quarantine Control in ISA Server 2004" document provides solutions for
- 888710 - Using ISA Server 2004 with Exchange Server 2003
- 888712 - Remote administration of Internet Security and Acceleration Server 2004
- 888714 - Outlook Web Access Server Publishing in ISA Server 2004
- 888716 - Digital Certificates for Internet Security and Acceleration Server 2004
- 888717 - Controlling secure Internet access by using ISA Server 2004
- 888042 - ISA Server 2004 does not support traffic redirection
- 888643 - The migration stops responding when you try to migrate configuration settings from an ISA Server 2000-based computer that uses SSL certificates to an ISA Server 2004-based computer
- 888711 - Site-to-site VPN in ISA Server 2004
- 888713 - VPN roaming clients and quarantine control in ISA Server 2004
- 841661 - You cannot install the Remote Access Quarantine Agent tool on your Windows 2000 Server-based computer
- 884506 - How to configure ISA Server 2004 to allow for RPC over HTTP client connections from Office Outlook 2003 to Exchange Server 2003
- 884580 - Active mode FTP client programs cannot access an FTP server from behind Internet Security and Acceleration Server 2004

- 886998 - Best practices when you publish two or more internal Web sites that use authentication on an Internet Security and Acceleration Server 2004-based computer
- 887002 - You experience a one-minute delay in the passage of ICMP ping traffic after you change the network relationship type for an IPSec site-to-site network rule in ISA Server 2004
- 887005 - Description of the time formats that are used in Internet Security and Acceleration Server 2004 log files and reports.
- 888649 - Core services that must be enabled for your Internet Security and Acceleration (ISA) Server 2004 computer to function correctly.
- 884496 - Client computers cannot access external resources and event ID 14147 appears in the Application log in ISA Server 2004
- 884560 - You cannot use the RADIUS authentication protocol when you use the OWA Forms-Based Authentication on a Web publishing rule to publish an internal Web site such as OWA in ISA Server 2004
- 885186 - How to publish a Web site directly on your Internet Security and Acceleration Server 2004 computer
- 884496 - Client computers cannot access external resources and event ID 14147 appears in the Application log in ISA Server 2004:
- 839509 - How to configure connectivity verifiers to monitor selected computers and networks in ISA Server 2004
- 884109 - How to enable VPN access for users in a front-end or back-end scenario in ISA Server 2004
- 884505 - How to use an ISA Server 2004 computer to block transparent HTTP clients without requiring authentication
- 885957 - How to install ISA Server 2004 hotfixes
- 884203 - VPN clients are disconnected when you restart the IPSec Policy Agent service on a computer that is running ISA Server 2004
- 884492 - The RADIUS authentication process in ISA Server 2004
- 884493 - A log query may not return all the results that you expect in Internet Security and Acceleration Server 2004
- 841665 - A network address translation IP address may be used for all outgoing network traffic on an ISA Server 2004 computer
- 884569 - The ISACTRL and WSPSRV services do not start when you install ISA Server 2004 on a multiprocessor computer
- 884495 - Event ID 7000 appears in the System log and the ISA Server Storage service does not start when you start a computer that is running ISA Server 2004
- 884494 - You receive a "Setup failed while registering Wspadmin.dll" error message when you try to install ISA Server 2004
- 883285 - Users are repeatedly prompted for their credentials when they try to access the Internet after you configure a firewall chain between ISA Server computers
- 884319 - ISA Server 2004 Standard Edition does not support NLB functionality
- 840472 - Internal DNS requests and internal LDAP requests may be sent to the external network adapter on a computer that is running ISA Server 2004
- 841664 - Clients may receive an "Error Code 500 Internal Server Error" error message if you use ISA Server 2004 to publish a Web site to a server that is on the internal network
- 838709 - How to use the ISA Server 2004 migration tool to migrate from ISA Server 2000 to ISA Server 2004
- 838378 - You cannot install ISA Server 2004 Administration Tools alongside ISA Server 2000 Administration Tools

- 837454 - How to configure access auditing for storage and for configuration in ISA Server 2000 and in ISA Server 2004